

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 9 月 1 7 日
Date of Application:

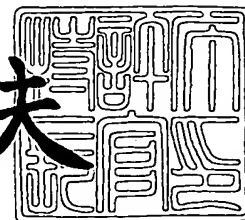
出 願 番 号 特 願 2 0 0 3 - 3 2 3 9 2 3
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 3 2 3 9 2 3]

出 願 人 株式会社ルネサステクノロジ
Applicant(s):

2 0 0 3 年 1 0 月 2 2 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康 夫



【書類名】 特許願
【整理番号】 R03001481
【提出日】 平成15年 9月17日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 12/14
【発明者】
 【住所又は居所】 東京都千代田区丸の内二丁目 4 番 1 号 株式会社ルネサステクノ
 ロジ内
 【氏名】 奥田 裕一
【特許出願人】
 【識別番号】 503121103
 【氏名又は名称】 株式会社ルネサステクノロジ
【代理人】
 【識別番号】 100089071
 【弁理士】
 【氏名又は名称】 玉村 静世
 【電話番号】 03-5217-3960
【先の出願に基づく優先権主張】
 【出願番号】 特願2002-362672
 【出願日】 平成14年12月13日
【手数料の表示】
 【予納台帳番号】 011040
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1

【書類名】 特許請求の範囲**【請求項 1】**

初期状態でスタティックラッチに第 1 状態を保持し、第 1 状態のスタティックラッチを構成する非導通状態の光検出用半導体素子に光が照射されて第 2 状態に反転する光ディテクタをメモリセルアレイに有し、前記光ディテクタによる光検出を内部動作の停止に利用することを特徴とする半導体集積回路。

【請求項 2】

前記非導通状態の光検出用半導体素子はスタティックラッチを構成する MOS トランジスタであることを特徴とする請求項 1 記載の半導体集積回路。

【請求項 3】

前記光検出用半導体素子としてダイオード素子を備え、前記ダイオード素子は前記 MOS トランジスタに並列に逆バイアス接続されることを特徴とする請求項 2 記載の半導体集積回路。

【請求項 4】

電流経路に直列に配置され動作可能な状態において導通状態にされる半導体素子と非導通状態にされる光検出用半導体素子を有し、非導通状態の光検出用半導体素子に光が照射されて変化する電流駆動力と導通状態の半導体素子の電流駆動力との比に応じて導通状態の半導体素子と非導通状態の光検出用半導体素子の接続点の電位が変化する光ディテクタを備え、前記光ディテクタによる光検出を内部動作の停止に利用することを特徴とする半導体集積回路。

【請求項 5】

前記非導通状態の光検出用半導体素子は MOS トランジスタであることを特徴とする請求項 4 記載の半導体集積回路。

【請求項 6】

前記非導通状態の光検出用半導体素子は前記電流経路に逆バイアス接続されるダイオード素子であることを特徴とする請求項 4 記載の半導体集積回路。

【請求項 7】

電流経路に感度調整用半導体素子を有する第 1 回路と、前記第 1 回路により光検出感度が調整され電流経路に光検出用半導体素子を有する第 2 回路と、第 2 回路の出力ノードレベルを検出する第 3 回路とを有し、前記光検出用半導体素子に光が照射されて電流変化を生ずる前記第 2 回路の出力ノードレベルに応じ前記第 3 回路の出力を変化させる光ディテクタを備え、前記光ディテクタによる光検出を内部動作の停止に利用することを特徴とする半導体集積回路。

【請求項 8】

前記光検出用半導体素子は前記電流経路を構成する MOS トランジスタであることを特徴とする請求項 7 記載の半導体集積回路。

【請求項 9】

前記光検出用半導体素子は、前記第 2 回路の電流経路の一部に並列配置されたダイオード素子であり、前記ダイオード素子は逆バイアス接続されることを特徴とする請求項 8 記載の半導体集積回路。

【請求項 10】

前記ダイオード素子は並列に複数個配置されることを特徴とする請求項 9 記載の半導体集積回路。

【請求項 11】

前記複数個のダイオード素子は半導体集積回路の半導体チップ上に遍在されていることを特徴とする請求項 10 記載の半導体集積回路。

【請求項 12】

メモリセルアレイにスタティック型メモリセルがマトリクス配置された S R A M モジュールを有し、前記 S R A M モジュールのメモリセルアレイに、一部のスタティック型メモリセルに代えて前記光ディテクタを配置したことを特徴とする請求項 1 記載の半導体集積回路。

路。

【請求項 13】

前記光ディテクタに代替された前記スタティック型メモリセルの欠損を補うことが可能な冗長構成を有することを特徴とする請求項 12 記載の半導体集積回路。

【請求項 14】

前記光ディテクタに代替された前記スタティック型メモリセルの欠損によって生ずるデータエラーの検出及び訂正が可能な ECC 回路を有することを特徴とする請求項 12 記載の半導体集積回路。

【請求項 15】

メモリセルアレイに書き換え不可能な不揮発性メモリセルがマトリクス配置されたマスク ROM を有し、前記マスク ROM のメモリセルアレイに、一部の不揮発性メモリセルに代えて前記光ディテクタが配置されたことを特徴とする請求項 1 記載の半導体集積回路。

【請求項 16】

メモリセルアレイに電氣的に書換え可能な不揮発性メモリセルがマトリクス配置されたフラッシュメモリを有し、前記フラッシュメモリのメモリセルアレイに、一部の不揮発性メモリセルに代えて前記光ディテクタが配置されたことを特徴とする請求項 1 記載の半導体集積回路。

【請求項 17】

クロック信号に同期動作される論理回路モジュールを有し、前記論理回路モジュールに前記光ディテクタが配置されることを特徴とする請求項 4 記載の半導体集積回路。

【請求項 18】

電源回路又はクロック発生回路を有し、前記電源回路又はクロック発生回路に前記光ディテクタが配置されることを特徴とする請求項 7 記載の半導体集積回路。

【請求項 19】

前記感度調整用半導体素子の電流駆動力を調整可能であることを特徴とする請求項 7 記載の半導体集積回路。

【請求項 20】

前記光検出用半導体素子における p n 接合部のうち、逆バイアス状態にされる p n 接合部の面積が他の接合部の面積よりも大きくされ、光に対する感度が同種の他の半導体素子よりも高いことを特徴とする請求項 1 乃至 19 の何れか 1 項記載の半導体集積回路。

【請求項 21】

前記光ディテクタの光検出用半導体素子以外の半導体素子の上層部を遮光する金属膜又はポリシリコン膜を有することを特徴とする請求項 1 乃至 20 の何れか 1 項記載の半導体集積回路。

【請求項 22】

前記光検出用半導体素子に逆方向接続のダイオードを並列接続することを特徴とする請求項 1、12、13 又は 14 に記載の半導体集積回路。

【請求項 23】

複数個の回路モジュールを有し、各回路モジュールにおいて前記光ディテクタはランダムに配置されることを特徴とする請求項 4 又は 7 記載の半導体集積回路。

【請求項 24】

複数個の回路モジュールを有し、各回路モジュールにおいて前記光ディテクタは規則的に配置されることを特徴とする請求項 4 又は 7 記載の半導体集積回路。

【請求項 25】

論理回路の基本素子と前記光ディテクタをペアとして備える基本セルが利用されたことを特徴とする請求項 4 記載の半導体集積回路。

【請求項 26】

前記基本セルを複数分散配置したことを特徴とする請求項 25 記載の半導体集積回路。

【請求項 27】

初期化状態でスタティックラッチに第 1 状態を保持し、第 1 状態のスタティックラッチを

構成する非導通状態の光検出用半導体素子に光が照射されて第2状態に反転する第1光ディテクタをメモリセルアレイに複数個有し、第1光ディテクタによる光検出信号を内部動作の停止に利用し、

電流経路に直列に配置され動作可能な状態において導通状態にされる半導体素子と非導通状態にされる光検出用半導体素子を有し、非導通状態の光検出用半導体素子に光が照射されて変化する電流駆動力と導通状態の半導体素子の電流駆動力との比に応じて導通状態の半導体素子と非導通状態の光検出用半導体素子との接続点の電位が変化する第2光ディテクタを論理回路モジュールに複数個有し、第2光ディテクタによる光検出を内部動作の停止に利用することを特徴とする半導体集積回路。

【請求項28】

電流経路に感度調整用半導体素子を有する第1回路と、前記第1回路により光検出感度が調整され電流経路に光検出用半導体素子を有する第2回路と、第2回路の出力ノードレベルを検出する第3回路とを有し、前記光検出用半導体素子に光が照射されて電流変化を生ずる前記第2回路の出力ノードレベルに応じ前記第3回路の出力を変化させる第3光ディテクタをアナログ回路に複数個備え、第3光ディテクタによる光検出を内部動作の停止に利用することを特徴とする請求項27記載の半導体集積回路。

【請求項29】

夫々の光ディテクタによる光検出信号の論理和信号を内部を初期化して動作を停止させるリセット信号とすることが可能なりセット回路を有することを特徴とする請求項1乃至28の何れか1項記載の半導体集積回路。

【請求項30】

カード基板に、外部インタフェース部と、前記外部インタフェース部に接続された請求項27又は28記載の半導体集積回路とを有することを特徴とするICカード。

【請求項31】

前記光検出信号の論理和信号の伝達経路にアクティブシールド配線が接続されることを特徴とする請求項29記載の半導体集積回路

【請求項32】

動作電圧の不所望な低下に応答して変化する電圧検出信号を出力する電圧検出回路と、前記電圧検出信号と前記夫々の光ディテクタによる光検出信号との論理和信号をリセット信号とすることが可能なりセット回路とを更に有することを特徴とする請求項1乃至28の何れか1項記載の半導体集積回路。

【請求項33】

内部クロック信号周波数の不所望な変化に応答して変化する周波数検出信号を出力する周波数検出回路と、前記周波数検出信号と前記夫々の光ディテクタによる光検出信号との論理和信号をリセット信号とすることが可能なりセット回路とを更に有することを特徴とする請求項1乃至28の何れか1項記載の半導体集積回路。

【請求項34】

所定の内部配線の切断に応答して変化する配線切断検出信号を出力する配線切断検出回路と、前記配線切断検出信号と前記夫々の光ディテクタによる光検出信号との論理和信号をリセット信号とすることが可能なりセット回路とを更に有することを特徴とする請求項1乃至28の何れか1項記載の半導体集積回路。

【請求項35】

光検出用半導体素子と、前記光検出用半導体素子以外の半導体素子の上層部を遮光する金属膜又はポリシリコン膜を有する光ディテクタとを備え、前記光検出用半導体素子は初期状態で非導通状態を保持し、非導通状態の前記光検出用半導体素子に光が照射されて導通状態に反転されて得られる前記光ディテクタによる光検出を内部動作の停止に利用することを特徴とする半導体集積回路。

【請求項36】

前記光ディテクタを複数分散配置したことを特徴とする請求項12、15、16又は35に記載の半導体集積回路。

【請求項 3 7】

電流経路に光検出用半導体素子を有する第 1 回路と、前記第 1 回路の出力ノードレベルを検出する第 2 回路とを備え、前記光検出用半導体素子に光が照射されて変化する電流に応じて前記第 1 回路の出力ノードが第 2 回路の論理閾値を跨ぐ光ディテクタを有し、前記光検出用半導体素子以外の半導体素子の上層部を遮光する金属膜又はポリシリコン膜が設けられ、前記光ディテクタによる光検出を内部動作の停止に利用することを特徴とする半導体集積回路。

【書類名】明細書

【発明の名称】半導体集積回路及びＩＣカード

【技術分野】

【0001】

本発明は、半導体集積回路及びＩＣカードに係り、例えばＩＣカード用マイクロコンピュータのような半導体集積回路が保有する暗号鍵等のリバースエンジニアリングの防止に適用して有効な技術に関する。

【背景技術】

【0002】

半導体技術の発展により、クレジットカード、有価証券等にＩＣ（Integrated Circuits）を組み込み、情報を暗号化して通信することで、安全で確実な決済を行うことが一般的になってきた。ＩＣを用いたこの方法は、従来の磁気記録を用いた方法に比べ、偽造、なりすまし等が困難であり、エンドユーザー、サービス提供者双方にメリットがある。

【0003】

暗号アルゴリズムについては長年研究が行われており、通信経路上で傍受した信号から、暗号鍵等を推定することは非常に困難であり、このリスクは事実上無視できる程小さい。問題はＩＣを開封し、リバースエンジニアリングを行うことで、ＩＣ上の内部情報や暗号鍵を直接読み出そうという試みである。リバースエンジニアリングとは、ハードウェアやソフトウェア製品に関して、構造や仕様を分析して技術的情報を明らかにするための技術、またはその行為を言う。

【0004】

従来は、ＩＣカードへ不正な周波数のクロックを供給したり、電源電圧を急激に上下させたり、強力な電磁波を照射したりで、ＩＣカードを異常動作させ、内部情報や暗号鍵を読み出すという手法が考案された。それに対し、ＩＣ側はそれらの異常な状態を検出することで、内部情報や暗号鍵を読み出されることを防いできた。

【0005】

例えば特許文献１には、ＩＣカード用ＩＣチップ内に開封センサを設け、開封を検出した場合にＣＰＵがメモリに対して消去動作を行って、機密保護に対する安全性を高める技術が記載される。

【0006】

特許文献２には、回路構成を封止及び遮光するパッケージの一部に光検出のセンサ部のみに光が照射されるように小窓を形成しておき、光の検出状態で通常に動作するとすると、不正解析を行う場合にはパッケージを開封し光の悪影響を避けるため暗所で解析が行われるため、光非検出状態では通常とは異なる動作が行なわれるようになり、この異なる動作故に動作解析を行うことができず、記憶情報の不正な読み出しも不可能にするという技術が記載される。

【0007】

特許文献３は、ＩＣに分散して複数の受光素子が集積され、複数の各受光素子が不揮発性メモリセルに接続された接続ライン、ロジック回路に接続された接続ライン或はロジックエレメントに接続された接続ラインの何れかの接続ラインに接続されて、この接続ラインを遮断し、導通し或は接地ラインに接続することにより接続ラインに関係する回路の正常な動作を阻害することでＩＣが開封されたときに内部情報を保護する技術を開示する。

【0008】

【特許文献１】特開平１０－３２０２９３号公報

【0009】

【特許文献２】特開２０００－２１６３４５号公報（段落０００９～００１１）

【特許文献３】特開平１１－１０２３２４号公報

【発明の開示】

【発明が解決しようとする課題】

【0010】

しかしながら、これらの文献は光の照射によって積極的に誤動作を誘発して統計的な手法で解析を試みるという新たなカードハッキングに対しては考慮されていない。本発明者はこれについて検討した。即ち、近年 IC カードへのリバースエンジニアリングの手法として、IC を開封し、強力な光を照射することで半導体素子の誤動作を誘発するという手法が提案されている。そのため、IC カード上に光を照射されたことを検出するセンサを設ける必要がある。

【0011】

一般的な IC に集積される半導体能動素子は、ダイオード、バイポーラトランジスタ、MOSFET（金属酸化膜半導体電界効果トランジスタ：Metal Oxide Semiconductor Field Effect Transistor）等が存在するが、いずれもその電圧・電流特性は p 型半導体と n 型半導体の境界である pn 接合の特性に大きく依存している。

【0012】

p 型半導体は電荷の移動に正の電荷を持つ正孔が支配的であり、n 型半導体は負の電荷を持つ自由電子が支配的である。正孔と自由電子は総称してキャリアと呼ばれている。pn 接合部では、正孔と自由電子が再結合するため、キャリアの存在確率が非常に低い、空乏層と呼ばれる領域が出現する。

【0013】

pn 接合において、p 型半導体の電位が高く、n 型半導体の電位が低い場合（順バイアスと呼ばれる）、p 型半導体中の正孔が電界により加速され空乏層へと流入する。同じく、n 型半導体中の自由電子も電界により加速され空乏層へと流入する。空乏層中では正孔と自由電子が再結合する。この現象は連続的に発生するため順バイアス時には電流が流れる。

【0014】

逆に p 型半導体の電位が低く、n 型半導体の電位が高い場合（逆バイアスと呼ばれる）、電界の向きが逆なので、p 型半導体中の正孔及び n 型半導体中の自由電子は空乏層に流れ込まない。また、空乏層中はキャリアがほとんど存在しないため、空乏層からキャリアが流出することも無い。このため逆バイアス時には電流がほとんど流れない。

【0015】

一般的に半導体論理回路では、バイポーラトランジスタや MOSFET をスイッチとして使用しており、逆バイアス状態の高抵抗が非導通状態（OFF）となる。ここで逆バイアス状態の空乏層に、光が入射された場合を考える。十分にエネルギーの大きい（波長の短い）光子が半導体中の価電子に衝突すると、価電子が励起され自由電子となり、電子が抜けて正の電荷を持った領域は正孔となる。すなわち光が入射する事で正孔・自由電子が対となって発生する。発生した正孔は電界により加速され、p 型半導体へ流出し、自由電子は n 型半導体へ流出する。光の入射が続く限り正孔・自由電子の発生が続くため、光が入射した場合 pn 接合の逆バイアスに電流が流れる事になる。

【0016】

空乏層にかかる電界が十分大きく、発生した正孔・自由電子対がほとんど再結合すること無しに、空乏層から流出するとすれば、電流の大きさは入射した光子の数に比例する事になる。すなわち、十分に強い光を入射する事で、OFF 状態の半導体スイッチ素子に、ON 状態の半導体スイッチ素子よりも大きな電流を流すことが出来、回路の誤動作を引き起こすことが出来る。このようにして、積極的に誤動作を誘発し、誤動作により本来出力されるべきでない情報が出力される可能性も有り、これを統計的な手法で解析を試みることによって、カードハッキングが可能にされることがある。

【0017】

本発明の目的は、光照射により積極的に誤動作を誘発して機密保護情報を不正に獲得するというカードハッキングに対する防御が可能な半導体集積回路、更には IC カードを提供することにある。

【0018】

本発明の前記並びにその他の目的と新規な特徴は本明細書の記述及び添付図面から明らかになるであろう。

【課題を解決するための手段】**【0019】**

本願において開示される発明のうち代表的なものの概要を簡単に説明すれば下記の通りである。

【0020】

〔1〕通常、ICが正常動作を行っていれば、内部情報や暗号鍵等が直接外部に出力されることが無いように設計されている。しかし、回路が誤動作を起こしている状態で、内部情報や暗号鍵等を完全に保護することは困難である。よって、光が照射されたことを検出し、回路の動作を停止する（例えばリセット指示により内部状態が初期化されてリセット指示が継続される）ことで内部情報や暗号鍵等が外部に出力されることを防ぐという手法が有効である。

【0021】

そのため、光ディテクタが必要となる。一般的に光を検出する半導体素子として、半導体撮像素子等に使用されるフォトダイオードが挙げられる。しかし一般的なロジックプロセスには、フォトダイオードが用意されないため、フォトダイオードを採用することはコストの増加につながる。また、フォトダイオードのような特殊な素子を使用することは、光ディテクタの位置を容易に把握されることにつながる。光ディテクタの位置さえ判明してしまえば、FIB (Field Ion Beam) による金属の堆積等で、光ディテクタをマスクすることが出来るため、防御手法としては弱い。

【0022】

またICカードのモバイル機器等への搭載を考えると、ICカード自体の消費電力は少なければ少ない程よい。光ディテクタは、通常動作時には特に目的が無いいため、できれば待機電力がほぼゼロであることが望ましい。

【0023】

そこで、ICカードマイコンなどの半導体集積回路に対し、（1）標準的なロジックプロセスで構成され、（2）他の回路と区別が付きにくく、（3）待機電力が極めて小さい、光ディテクタを搭載することにより、光の照射によるリバースエンジニアリングを効果的に防ごうとするものである。そのために以下の手段を講ずる。

【0024】

〔2〕（スタティックラッチ型）本発明に係る半導体集積回路は、初期状態でスタティックラッチに第1状態を保持し、第1状態のスタティックラッチを構成する非導通状態の半導体素子に光が照射されて第2状態に反転する光ディテクタをメモリセルアレイに複数個有し、光ディテクタによる光検出信号を内部動作の停止に利用する。スタティックラッチ型の光ディテクタをメモリアレイに組み込むことで、光ディテクタを目立たずに配置することができる。

【0025】

本発明の具体的な形態として、前記非導通状態の光検出用半導体素子はスタティックラッチを構成するMOSトランジスタである。また、前記光検出用半導体素子としてダイオード素子を備え、前記ダイオード素子は前記MOSトランジスタに並列に逆バイアス接続される。

【0026】

最適な形態として、メモリセルアレイにスタティック型メモリセルがマトリクス配置されたSRAMモジュールを有するとき、前記SRAMモジュールのメモリセルアレイに一部のスタティック型メモリセルに代えて前記光ディテクタを複数個分散配置する。

【0027】

光ディテクタが存在する部分にはメモリセルが無くなるが、前記光ディテクタに代替されたスタティック型メモリセルの欠損を補うことが可能な冗長構成を利用することができ

る。或は、前記光ディテクタに代替されたスタティック型メモリセルの欠損によって生ずるデータエラーの検出及び訂正が可能な ECC 回路を利用すればよい。

【0028】

(プッシュ・プル型) 第2の観点による半導体集積回路は、電流経路に直列に配置され動作可能な状態において導通状態にされる半導体素子と非導通状態にされる光検出用半導体素子を有し、非導通状態の光検出用半導体素子に光が照射されて変化する電流駆動力と導通状態の半導体素子の電流駆動力との比に応じて導通状態の半導体素子と非導通状態の光検出用半導体素子の接続点の電位が変化する光ディテクタを複数個有し、光ディテクタによる光検出を内部動作の停止に利用する。この種の光ディテクタはクロック信号に同期動作される論理回路モジュールに適用して、複数個を分散配置するのがよい。プッシュ・プル型の光ディテクタはロジック回路に対して目立たずその存在位置は容易に悟られない。

【0029】

本発明の具体的な形態として前記非導通状態の光検出用半導体素子は例えば MOS トランジスタである。また、前記非導通状態の光検出用半導体素子は前記電流経路に逆バイアス接続されるダイオード素子である。

【0030】

(感度差型) 第3の観点による半導体集積回路は、電流経路に感度調整用半導体素子を有する第1回路と、前記第1回路により光検出感度が調整され電流経路に光検出用半導体素子を有する第2回路と、第2回路の出力ノードレベルを検出する第3回路とを有し、前記光検出用半導体素子に光が照射されて電流変化を生ずる前記第2回路の出力ノードレベルに応じ前記第3回路の出力を変化させる光ディテクタを複数個有し、光ディテクタによる光検出を内部動作の停止に利用する。望ましい態様として、電源回路及びクロック発生回路に複数個の前記光ディテクタを分散配置するのがよい。感度差型の光ディテクタは常時貫通電流を流す回路形式故にアナログ的回路の内部に配置してもその所在は容易に知り得ない。望ましい態様として、前記感度調整用半導体素子の電流駆動力を調整可能にするのがよい。検出感度の修正もしくは最適化が容易になる。

【0031】

本発明の具体的な形態では、例えば前記光検出用半導体素子は前記電流経路を構成する MOS トランジスタである。また、前記光検出用半導体素子は前記第2回路の電流経路の一部に並列配置されたダイオード素子であり、前記ダイオード素子は逆バイアス接続される。前記ダイオード素子を並列に複数個配置すれば光検出は更に確実になる。この意味において、前記複数個のダイオード素子は半導体集積回路の半導体チップ上に偏在されるのがよい。

【0032】

(光検出動作の確実化) 光照射により専ら光検出素子の電流駆動力もしくは電流量を他の素子と区別可能に増大させるには、前記光検出用半導体素子における p n 接合部のうち、逆バイアス状態にされる p n 接合部の面積を他の接合部の面積よりも大きくし、光に対する感度が同種の他の半導体素子よりも高いようにすればよい。或は、光検出用半導体素子以外の半導体素子の上層部を遮光する金属膜又はポリシリコン膜を採用すればよい。また、前述のように、前記光検出用半導体素子として MOS トランジスタに逆方向バイアスのダイオードを並列接続した構成などを採用したり、前記スタティックラッチを電流リミッタ半導体素子を介して電源電位及び回路の接地電位に接続したりする構成によっても、光検出動作の確実化に資することができる。

【0033】

(光ディテクタの配置) 各回路モジュールにおいて前記光ディテクタは基本セルのレイアウトで生じた隙間に配置してよい。結果として、各回路モジュールにおいて前記光ディテクタはランダムに配置される。

【0034】

また、各回路モジュールに基本セルをレイアウトする前に、予め、各回路モジュールに

において前記光ディテクタを規則的なパターン例えば格子状を描いて配置する。先に光ディテクタを規則的に配置するから光ディテクタの密度調整が可能になる。但し、基本セル間に余計な隙間が発生し、チップ占有面積増大の傾向を採ることになる。

【0035】

光ディテクタを容易に高密度配置できるようにするには、論理回路の基本素子と前記光ディテクタをペアとして備える基本セルを利用するのがよい。

【0036】

(回路モジュールに対する光ディテクタの最適化) 本発明の別の観点による半導体集積回路は、初期状態でスタティックラッチに第1状態を保持し、第1状態のスタティックラッチを構成する非導通状態の半導体素子に光が照射されて第2状態に反転する第1光ディテクタをメモリセルアレイに複数個有し、第1光ディテクタによる光検出信号を内部動作の停止に利用し、また、電流経路に直列に配置され動作可能な状態において導通状態にされる半導体素子と非導通状態にされる半導体素子を有し非導通状態の半導体素子に光が照射されて変化する電流駆動力と導通状態の半導体素子の電流駆動力との比に応じて導通状態の半導体素子と非導通状態の半導体素子の接続点の電位が変化する第2光ディテクタを論理回路モジュールに複数個有し、第2光ディテクタによる光検出信号を内部動作の停止に利用する。

【0037】

更に、電流経路に感度調整用半導体素子を有する第1回路と、電流経路に光検出用半導体素子を有する第2回路と、第2回路の出力ノードレベルを検出する第3回路とを有し、前記光検出用半導体素子に光が照射されて変化する電流に応じて前記第2回路の出力ノードが第3回路の論理閾値を跨ぐ第3光ディテクタをアナログ回路に複数個有し、光ディテクタによる光検出信号を内部動作の停止に利用する。

【0038】

夫々の光ディテクタによる光検出信号の論理和信号をリセット信号とすることが可能なリセット回路を有する。光検出の度にリセットがかかれば、積極的に誤動作を誘発して機密保護情報を不正に獲得することは難しくなる。

【0039】

本発明に係るICカードは、カード基板に、外部インタフェース部と、前記外部インタフェース部に接続された上記半導体集積回路とを有する。

【発明の効果】

【0040】

本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば下記の通りである。

【0041】

すなわち、スタティックラッチのオフ状態で安定している半導体素子に光を照射することで、当該スタティックラッチが反転する事を利用して、光ディテクタを構成することができる。スタティックラッチ型の光ディテクタをメモリアレイの中に組み込むことで、光ディテクタを目立たずに配置することが出来る。その時、光ディテクタが存在する部分にはメモリセルがなくなるが、冗長或はECC回路を用いて正常なメモリ機能を保証することができる。

【0042】

プッシュ・プル型回路の非導通半導体素子に光を照射して出力を反転可能にする構成を光ディテクタに採用すれば、それを目立たずにロジック回路に配置することができる。

【0043】

電流経路に配置された感度調整用半導体素子に流れる電流に対して光検出用半導体素子に光が照射されて変化する電流に応じて出力を変化させる構成を光ディテクタに採用すれば、それを目立たずに電源回路等のアナログ回路やクロック発生回路に配置することができる。

【0044】

光ディテクタの光検出用半導体素子を金属等で覆うことにより、光ディテクタの動作をより確実にすることができる。光ディテクタの感度調整は、光検出用の半導体素子の逆バイアス p n 接合部の面積調整、ダイオードの追加、電流制限、光検出 MOS トランジスタとの電流を比較する MOS トランジスタの W/L 調整等で行うことができる。

【0045】

上記半導体集積回路を IC カードなどに採用することにより、積極的に半導体集積回路の誤動作を誘発して機密保護情報を不正に獲得するというカードハッキングに対する防御が可能になる。

【発明を実施するための最良の形態】

【0046】

図1に本発明の第1実形態である、SRAM型光ディテクタ100を示す。図1に示した通りSRAM型光ディテクタ100は、6トランジスタ型SRAMメモリセルと同様の構成となっている。即ち、pチャンネル型MOSトランジスタ113, 114とnチャンネル型MOSトランジスタ111, 112から成るスタティックラッチ120を主体に、その一方の入出力ノードがnチャンネル型トランスファMOSトランジスタMOS115を介して電源電位VDDに、他方の入出力ノードがnチャンネル型トランスファMOSトランジスタMOS116を介して回路の接地電位VSSに接続され、双方のトランスファMOSトランジスタ115, 116はリセット信号101によりスイッチ制御されるように構成される。

【0047】

一般的なICカードは、CPU（中央演算処理装置：Central Processing Unit）、SRAM（Static Random Access Memory）、ROM（Read Only Memory）、EEPROM（Electrical Erasable Programmable ROM）等を1チップに集積したSOC（System On Chip）によって構成される。よって、ICカード用の製造プロセスでSRAMを構成することができ、SRAM領域にSRAM型光ディテクタ100を配置することで、光ディテクタの存在が目立たなくなる。言うまでもなく、光ディテクタ100の待機時電力はほぼゼロである。

【0048】

前記SRAM型光ディテクタ100の動作について説明する。まずICカードに電源が投入された時点で、101はリセット信号に繋がっていて、パワーオンリセットの働きで、リセット信号101がハイレベル（Hi）になり、トランスファMOSトランジスタ115, 116がオンになる。トランスファMOSトランジスタ115のソースは電源電位VDDに接続、トランスファMOSトランジスタ116のソースは接地電位VSSに接続されているため、センサ出力102の電位はローレベル（Lo）に、ノード103の電位はHiにリセットされる。この時、MOSトランジスタ111, 114はオン、MOSトランジスタ112, 113はオフ状態となる。オフ状態のMOSトランジスタ112, 113に光が入射する事で、MOSトランジスタ112, 113がオンとなる。入射する光子の数が十分多くMOSトランジスタ112, 113の抵抗がMOSトランジスタ111, 114の抵抗を下回れば、前記スタティックラッチ120が反転し、ノード103がLoに、センサ出力102の電位はHiに遷移する。この動作により光の照射を検出することができる。

【0049】

図1の例では6トランジスタ型SRAMメモリセルを基にした光ディテクタを示したが、SRAMメモリセルには他にも抵抗負荷を用いた4トランジスタ型を始めとしてさまざまな形式が提案されている。言うまでもないことであるが、SRAMメモリセルの形式に拘わらず、オフになっているMOSトランジスタに光が入射してスタティックラッチ120が反転するという条件を満足する如何なる構成によっても、光ディテクタを構成することが可能である。

【0050】

MOSトランジスタ112, 113に入射したのと同じだけの光子数が、MOSトランジスタ111, 114にも入射した場合、MOSトランジスタ111, 114にも電流が流れスタティックラッチ120は反転しにくくなる。これを防ぐにはいくつかの方法が考えられる。一つには、MOSトランジスタ111, 114の上層を金属で覆ってしまうという方法である。図2にSRAM型光ディテクタ100のレイアウト概略図を示す。一般的に6トランジスタ型SRAMメモリセルはレイアウト面積を削減するために、図2のような配置にする。この時、ハッチングで示した部分の上層を金属で覆うことにより、MOSトランジスタ112, 113以外に光子が入射する事はない。

【0051】

直接遮光するほかに、MOSトランジスタの光に対する感度を変化させることもできる。図3にオフ状態のnチャンネル型MOSトランジスタ300を示す。301はp型ウェル拡散領域、302はドレイン拡散領域、303はソース拡散領域、304はウェル給電拡散領域、311はドレイン端子、312はゲート端子、313はソース端子、314は基板端子、320は入射する光子である。各端子はゲート端子312、ソース端子313、基板端子314が接地電位VSSであり、ドレイン端子が電源電位VDDとなり、本MOSトランジスタ300はオフとなっている。

【0052】

半導体に十分なエネルギーを持った光子が入射すると、正孔・自由電子対が発生する。逆バイアス状態のpn接合に正孔・自由電子対が発生した場合には、発生したキャリアにより、逆バイアスにも電流が流れる。図3において、p型ウェル拡散領域301とドレイン拡散領域302のpn接合が逆バイアスになっている。よって、オフ状態のnチャンネル型MOSトランジスタ300に光子320が入射する事による漏れ電流は、主にドレイン311から基板314へ流れる。図3はnチャンネル型MOSトランジスタであるがpチャンネル型MOSトランジスタの場合も同様である。

【0053】

そこで、前記MOSトランジスタ112、113のドレイン拡散面積を広くレイアウトする。ドレイン拡散面積を広くすることによりpn接合部の空乏層領域が拡大し、光子が一樣に入射するとすれば、ドレイン面積が大きければそれだけ漏れ電流が大きくなる。よって、MOSトランジスタ111, 114と比較してMOSトランジスタ112, 113のドレイン面積を大きくレイアウトすれば、同様な光がMOSトランジスタ111~114へ入射したとしても、よりスタティックラッチ120が反転しやすくなる。

【0054】

もちろん言うまでもないことであるが、金属による遮光とドレイン面積の増大を併用することは可能である。

【0055】

図4に前記SRAM型光ディテクタ100の配置の例を示す。ICカード上のSRAMブロック400は、図4のように、メモリセルアレイ401、冗長セルアレイ402、冗長プログラム回路403、ロウデコーダ404、カラムデコーダ405、カラムスイッチアレイ406、ECC (error correcting cord) 回路407、センスアンプ408、ライトアンプ409及びタイミングジェネレータ410を有して成る。メモリセルアレイ401はマトリクス配置されたスタティックメモリセルを有し、スタティックメモリセルの選択端子は行毎にワード線WLに接続され、スタティックメモリセルのデータ入出力端子は列毎にビット線BLに接続される。ロウデコーダ404はロウアドレス信号RADRをデコードしてワード線選択信号を形成する。相補ビット線BLはカラムスイッチアレイ406のスイッチを介してコモンデータ線CDに接続可能される。カラムアドレスデコーダはカラムアドレス信号CADRをデコードしてコモンデータ線CDに導通させるべき相補ビット線BLをカラムスイッチアレイ406のスイッチを用いて選択する。

【0056】

センスアンプ408はメモリセルからコモンデータ線CDに読み出された記憶情報をセ

ンスしてECC回路407に供給する。ライトアンプ409はメモリセルへの書き込み情報に従ってコモンデータ線CDをドライブする。

【0057】

前記ECC回路407は外部からの書き込みデータにECCコードを付加して、これを書き込み情報として書き込みアンプ409に供給し、また、センスアンプ408からコモンデータ線CDに読み出された読み出し情報を入力してこれに付随するECCコードを用いて読み出しデータに誤りが有るかを判別し、誤りが有ればこれを訂正して出力する。

【0058】

前記冗長セルアレイ402はメモリセルアレイ401の不良ビットを救済するための冗長メモリセルを有し、不良ビットをワード線単位又は相補ビット線単位で置き換え可能にされる。ワード線単位又は相補ビット線単位の置き換えるべき不良アドレスは冗長プログラム回路403に設定され、設定された不良アドレスにアクセスアドレスが一致したとき、ワード線又はビット線の置き換えが行なわれる。尚、冗長構成それ自体については既に公知であるからここではその詳細について説明を省略する。

【0059】

図4のメモリセルアレイ401において、枠目は一つ一つがSRAMのスタティックメモリセル（単にSRAMセルとも記す）を示している。このうち斜線で示したSRAMセルを、SRAM型光ディテクタ100で置き換える。図4のようにSRAM型光ディテクタ100をランダムに配置することで、リバースエンジニアリングをより困難にすることができる。

【0060】

メモリセルアレイ401において前記夫々のSRAM型光ディテクタ100はメモリセルのワード線及びビット線とは接続されず、ビット線とは異なる信号配線を用いて前記光検出信号102をSRAMモジュールの外部に出力するようになっている。複数のSRAM型光ディテクタ100の夫々の前記光検出信号102はワイアード・オア接続或はオアゲートを介して外部に出力されればよい。

【0061】

SRAMセルをSRAM型光ディテクタ100に置き換えることで、そのSRAMセルはメモリセルとしては使用できなくなり、これによってSRAMとしての機能に問題が生じてはならない。そこで、前記冗長用の冗長セルアレイ402と冗長プログラム回路403を利用する。即ち、SRAM型光ディテクタ100を、冗長セルアレイ402のメモリセルで代替することで、SRAMとしての機能を損なわずに、SRAM型光ディテクタ100を配置することができる。或は、冗長用の構成を利用しなくても、前記ECC回路407を利用することにより、読み出し時にSRAM型光ディテクタ100に置き換えられたビットラインは不定になるが、センスアンプ408からはHレベルかLレベルが出力されることにより、メモリセルの欠落によって生ずる誤りを訂正して対処することができる。冗長を用いて光ディテクタ素子を代替しなくても済む。また、SRAM型光ディテクタ100に対する置き換えがメモリセルの欠陥救済に影響を与えないことがない。ECCによる誤り訂正を可能にするには、SRAM型光ディテクタ100はECC回路による誤り訂正能力以下になるように分散配置されることが必要である。

【0062】

図5に第2例である、ダイオード追加SRAM型光ディテクタ500を示す。ダイオード追加SRAM型光ディテクタ500は、SRAM型光ディテクタ100のMOSトランジスタ112、113に並列にダイオード511、512を追加したものである。遮光を行う場合は、ダイオード511、512にも光が当たるようにする。なお、特に制約を受けるものではないが、ダイオード511はn型ウェル領域のp型拡散層で構成され、ダイオード512はp型ウェル領域のn型拡散層で構成されるものとする。

【0063】

基本的な動作は、SRAM型光ディテクタ100と同様であるため省略する。追加したダイオードは、MOSトランジスタ112、113のドレイン・基板のpn接合に並列し

たpn接合である。そのため、MOSトランジスタ112, 113のドレイン面積を増加したものと同様の効果を持つ。ダイオードとして独立させることで、レイアウトの自由度が増し、ドレイン面積増大では対応できないほど大きなpn接合を持たせることも可能である。また、SRAMスタティックラッチ120とダイオードが近接して配置している必要は必ずしも無いため、ダイオード511, 512を分離してレイアウトすることで、さらにレイアウトの自由度を増やすとができる。

【0064】

図6に第3例である、電流リミッタ追加SRAM型光ディテクタ600を示す。電流リミッタ追加SRAM型光ディテクタ600は、ダイオード追加SRAM型光ディテクタ500におけるSRAMラッチの電源電位VDD及びグラウンドVSSに、電流リミッタMOSトランジスタ611, 612を追加したものである。

【0065】

電流リミッタ追加SRAM型光ディテクタ600の動作について説明する。まず、SRAM型光ディテクタ100と同様、パワーオンリセットの働きで、リセット信号101がHiになり、トランスファMOSトランジスタ115, 116がオンになる。トランスファMOSトランジスタ115のソースは電源電位VDDに接続、トランスファMOSトランジスタ116のソースは接地電位VSSに接続されているため、センサ出力102の電位はLoに、ノード103の電位はHiにリセットされる。この時、MOSトランジスタ111, 114はオン、MOSトランジスタ112, 113はオフ状態となる。オフ状態のMOSトランジスタ112, 113に光が入射する事で、MOSトランジスタ112, 113がオンとなる。この時、MOSトランジスタ111, 114はオン状態のため、スタティックラッチ120を構成するMOSトランジスタ111~114の全てに電流が流れ、スタティックラッチ120に直流電流が発生する。直流電流が流れることで、電流リミッタMOSトランジスタ611のドレイン電位が上がり、電流リミッタMOSトランジスタ612のドレイン電位が下がる。この効果によりスタティックラッチ120の電源電圧が低下し、ラッチが反転しやすくなる。すなわち光子数に対する光ディテクタの感度が増加するということである。SRAM型光ディテクタ100及び、ダイオード追加SRAM型光ディテクタ500の光感度は、基本的にpn接合面積で調整するが、本電流リミッタ追加SRAM型光ディテクタ600の感度は、電流リミッタMOSトランジスタ611, 612の電流駆動力で調整することができ、設計が容易になる。

【0066】

以上、SRAMセルを基にした光ディテクタの構成について説明してきた。SRAMは、ICカードの中でもワークエリアとして使用され、リバースエンジニアリングの標的とされることが多い。よってSRAMアレイに光ディテクタを埋め込み、リバースエンジニアリングを困難にすることは重要である。他にも、CPU部のフリップフロップ等に誤動作を誘発し、リバースエンジニアリングを行うという手法も考えられる。それを防ぐためには、標準ロジックセルの規格に従った（セル高さ、幅等）光ディテクタがあれば都合が良い。もちろんSRAM型光ディテクタを、標準ロジックセルの規格に従いレイアウトすれば問題ないが、より標準ロジックセルに適合した回路形式があればなお良い。以下、標準ロジックセルの規格に合わせてレイアウトすることを前提とした光ディテクタの構成について説明する。

【0067】

図7に第4例である、インバータ型光ディテクタ700を示す。701は負論理イネーブル信号、702はディテクタ出力信号、703はセンサ信号、711は感度調整MOSトランジスタ、712は光検出MOSトランジスタ、713は出力インバータ、VDDは電源電位、VSSはグラウンド電位である。

【0068】

インバータ型光ディテクタ700は負論理イネーブル信号701がLoに落ち、感度調整MOSトランジスタ711がオンになることで起動する。光子が入射していない場合、光検出MOSトランジスタ712のゲート・ソースが短絡されているため、光検出MOS

トランジスタ712はオフである。よって光子が入射していない場合、センサ信号703は電源電位、ディテクタ出力702はグラウンド電位VSSである。光検出MOSトランジスタ712に光子が入射すると電流が流れ、電流駆動力の比によりセンサ信号703が低下する。光子数が一定以上となり、センサ信号703の電位が出力インバータ713の論理スレッシュホールド（論理閾値電圧）を下回ると、ディテクタ出力702がHiとなり、光が検出される。

【0069】

図8に第5例である、バイアストインバータ型光ディテクタ800を示す。801は負論理イネーブル信号、802は正論理イネーブル信号、803はバイアスノード、804はセンサ信号、805はディテクタ出力信号である。811, 815, 819はpチャンネル型電流制限MOSトランジスタである。814, 818, 822はnチャンネル型電流制限MOSトランジスタである。813, 821はnチャンネル型感度制御MOSトランジスタ、817はnチャンネル型光検出MOSトランジスタである。これらの素子のうち、光を当てるのは光検出MOSトランジスタ817のみで、他の素子は金属膜で覆いをする。ここでMOSトランジスタのW, Lの値は、 $811=815=819$ 、 $812=816=820$ 、 $813=821$ 、 $814=818=822$ と設計される。

【0070】

負論理イネーブル信号801がHi、正論理イネーブル信号802がLoの時、バイアストインバータ型光ディテクタ800はオフである。MOSトランジスタ811, 814, 815, 818によって電流が流れなくなり、センサ信号804はMOSトランジスタ823によりプルアップされ、ディテクタ出力信号805はグラウンド電位VSSで固定される。

【0071】

負論理イネーブル信号801がLo、正論理イネーブル信号802がHiに切り替わると、バイアストインバータ型光ディテクタ800が起動し、MOSトランジスタ811～814によって構成されるクロックドインバータ型のバイアス回路のネガティブフィードバックによりバイアスノード803の電位が決定する。この時、MOSトランジスタのW, Lの値は、 $811=819$ 、 $812=820$ 、 $813=821$ 、 $814=822$ と設計されているため、バイアスノード803の電位はMOSトランジスタ819～822によって構成されるインバータの論理スレッシュホールドに等しい。ここでもしMOSトランジスタ813=817と設計されていれば、センサ信号804の電位もバイアスノード803の電位と等しくなるはずである。実際のW/Lの値はMOSトランジスタ813>817と設計しておく。短チャネル効果の影響をなくすため、Lを等しくWの値を813>817と設計することが望ましい。このように設計を行うことで、MOSトランジスタ813と817の電流駆動力の違いからセンサ信号804の電位は、バイアスノード803の電位より高くなり、ディテクタ出力信号805はグラウンド電位付近で安定する。

【0072】

光検出MOSトランジスタ817に光子が入射すると、光検出MOSトランジスタ817のドレイン・基板間に漏れ電流が発生する。すると電流が増加するため、センサ信号804の電位が低下する。光子数が増加しセンサ信号804の電位が、MOSトランジスタ819～822によって構成されるインバータの論理スレッシュホールドを下回った時、ディテクタ出力信号805はHiに遷移する。

【0073】

本バイアストインバータ型光ディテクタ800の特徴は、nチャンネル型MOSトランジスタ813（=821）と817のW/Lの差により光検出の感度を容易に調整できることである。本バイアストインバータ型光ディテクタ800が動作している間は、常に電流が流れつづけるが、pチャンネル型電流制限MOSトランジスタ811, 815, 819、及びnチャンネル型電流制限MOSトランジスタ814, 818, 822のW/Lの値を小さく設定することで、ICカード全体の消費電力と比較して問題にならない程度に低消費電力化することが可能である。

【0074】

図9に第6例である、カレントミラー型光ディテクタ900を示す。901は負論理イネーブル信号、902は正論理イネーブル信号、903はバイアスノード、904はセンサ信号、905はディテクタ出力信号、911はpチャンネル型電流源MOSトランジスタ、913はnチャンネル型バイアスMOSトランジスタである。915, 917はカレントミラーを構成するMOSトランジスタ、916はnチャンネル型感度調整MOSトランジスタ、919はnチャンネル型光検出MOSトランジスタ、920~923は電流制限インバータ、912はnチャンネル型プルダウンMOSトランジスタである。914, 918はpチャンネル型プルアップMOSトランジスタである。これらの素子のうち、光を当てるのは光検出MOSトランジスタ919のみで、他の素子は金属膜で覆いをする。

【0075】

負論理イネーブル信号901がHi、正論理イネーブル信号902がLoの時、カレントミラー型光ディテクタ900はオフである。プルダウンMOSトランジスタ912により、MOSトランジスタ913, 916, 919に電流が流れなくなり、センサ信号904はプルアップMOSトランジスタ918によりプルアップされ、ディテクタ出力信号905はグラウンド電位VSSで固定される。

【0076】

負論理イネーブル信号901がLo, 正論理イネーブル信号902がHiに切り替わると、カレントミラー型光ディテクタ900が起動する。電流源MOSトランジスタ911に流れる電流が、バイアスMOSトランジスタ913に流れ、バイアスノード903の電位が決定する。ここで感度調整MOSトランジスタ916と光検出MOSトランジスタ919のW, Lが同一であれば、2つのMOSトランジスタには同一の電流が流れる。実際は感度調整MOSトランジスタのWを大きくし、感度調整MOSトランジスタ916のほうに大きな電流が流れるように設計される。2つのMOSトランジスタの電流差は、MOSトランジスタ915, 917で構成されるカレントミラー能動負荷で増幅される。MOSトランジスタ915, 917のチャネル長変調係数が十分小さいとすれば、センサ出力904は電源電位VDD付近で、ディテクタ出力信号905はグラウンド電位VSS付近で安定する。

【0077】

光検出MOSトランジスタ919に光子が入射すると、光検出MOSトランジスタ919のドレイン・基板間に漏れ電流が発生する。すると電流が増加する。光検出MOSトランジスタ919に流れる電流が、感度調整MOSトランジスタ916に流れる電流を上回ると、カレントミラー能動負荷の働きで、センサ信号904の電位がグラウンド電位VSS付近まで下がる。その結果ディテクタ出力信号905はHiレベルに遷移し、光の照射が検出される。

【0078】

本カレントミラー型光ディテクタ900もまた、感度調整MOSトランジスタ916と光検出MOSトランジスタ919とのW/Lの差により光感度を容易に調整可能である。この回路も動作中は常に電流が流れるが、MOSトランジスタ911と913で構成されるバイアス回路と、出力インバータに電流を制限するMOSトランジスタ920, 923のW, L値を適宜調整することで、ICカード全体の消費電力に対して問題にならない程度に低消費電力化することができる。

【0079】

図10に第7例である、ディファレンシャルAMP型光ディテクタ1000を示す。1001は負論理イネーブル信号、1002は正論理イネーブル信号、1003はバイアスノード、1004はセンサ信号、1005はディテクタ出力信号、1011はpチャンネル型電流源MOSトランジスタ、1013はnチャンネル型バイアスMOSトランジスタ、1024はnチャンネル型電流源MOSトランジスタである。1015, 1017はカレントミラー負荷を構成するMOSトランジスタ、1016はnチャンネル型感度調整MOSトランジスタ、1019はnチャンネル型光検出MOSトランジスタ、1020~1

023は電流制限インバータ、1012はnチャンネル型プルダウンMOSトランジスタである。1014、1018はpチャンネル型プルアップMOSトランジスタである。これらの素子のうち、光を当てるのは光検出MOSトランジスタ1019のみで、他の素子は金属膜で覆いをする。

【0080】

負論理イネーブル信号1001がHi、正論理イネーブル信号1002がLoの時、デифференシャルAMP型光ディテクタ1000はオフである。プルダウンMOSトランジスタ1012により、電流源MOSトランジスタ1024に電流が流れなくなり、センサ信号1004はプルアップMOSトランジスタ1018によりプルアップされ、ディテクタ出力信号1005はグラウンド電位VSSで固定される。

【0081】

負論理イネーブル信号1001がLo、正論理イネーブル信号1002がHiに切り替わると、デифференシャルAMP型光ディテクタ1000が起動する。電流源MOSトランジスタ1011に流れる電流が、バイアスMOSトランジスタ1013に流れ、カレントミラーにより電流源MOSトランジスタ1024の電流が決定する。ここで感度調整MOSトランジスタ1016と光検出MOSトランジスタ1019のW、Lが同一であれば、2つのMOSトランジスタには同一の電流が流れる。実際は感度調整MOSトランジスタのWを大きくし、感度調整MOSトランジスタ1016の方に大きな電流が流れるように設計される。2つのMOSトランジスタの電流差は、MOSトランジスタ1015、1017で構成されるカレントミラー能動負荷で増幅される。MOSトランジスタ1015、1017のチャネル長変調係数が十分小さいとすれば、センサ出力1004は電源電位VDD付近で、ディテクタ出力信号1005はグラウンド電位VSS付近で安定する。

【0082】

光検出MOSトランジスタ1019に光子が入射すると、光検出MOSトランジスタ1019のドレイン・基板間に漏れ電流が発生する。すると電流が増加する。光検出MOSトランジスタ1019に流れる電流が、感度調整MOSトランジスタ1016に流れる電流を上回ると、カレントミラー能動負荷の働きで、センサ信号1004の電位がグラウンド付近まで下がる。その結果ディテクタ出力信号1005はHiレベルに遷移し、光の照射が検出される。

【0083】

本デифференシャルAMP型光ディテクタ1000の特徴も、カレントミラーAMP型光ディテクタ900等と同様、感度調整MOSトランジスタ1016と光検出MOSトランジスタ1019とのWの差により光感度を容易に調整可能な事である。さらに、カレントミラーAMP型光ディテクタ900等と比較して、光検出MOSトランジスタ1019のドレイン電位が高くなるのが利点としてあげられる。各光ディテクタは、光検出MOSトランジスタのドレイン・基板間のpn逆バイアスに発生する漏れ電流を検出することで、光の入射を検出している。ドレイン電位が低い場合、空乏層中の電界が弱く、光子の入射によって発生した正孔・自由電子対が空乏層を抜ける前に再結合する確率が上がってしまう。デифференシャルAMP型光ディテクタ1000は、光検出MOSトランジスタ1019のドレイン電位を上げることで、ドレイン・基板間の電界を強化し、より光感度を上昇させている。デифференシャルAMP型光ディテクタ1000もまた、動作中に電流が常に流れるが、MOSトランジスタ1011と1013で構成されるバイアス回路と、出力インバータに電流を制限するMOSトランジスタ1020、1023のW、L値を適宜調整することで、ICカード全体の消費電力に対して問題にならない程度に低消費電力化することができる。

【0084】

図11には図8のバイアストインバータ型光ディテクタ800の変形例が示される。図11に示されるバイアストインバータ型光ディテクタ800Aは、感度制御用素子の電流駆動能力を調整可能にしたものである。即ち、感度制御MOSトランジスタ813aと電流制限MOSトランジスタ814aの直列回路、感度制御MOSトランジスタ813bと

電流制限MOSトランジスタ814bの直列回路、及び感度制御MOSトランジスタ813cと電流制限MOSトランジスタ814cの直列回路を並列に配置した点が図8の構成と相違される。MOSトランジスタのW, Lの値は、 $814a = 814b = 814c = 814$ である。MOSトランジスタ813a, 813b, 813cのLはMOSトランジスタ817と同じで、MOSトランジスタ813a, 813b, 813cの W_{813a} , W_{813b} , W_{813c} は、MOSトランジスタ817の W_{817} に対して、例えば、 $W_{813a} = 3 \cdot W_{817} / 4$, $W_{813b} = 1 \cdot W_{817} / 8$, $W_{813c} = 1 \cdot W_{817} / 16$ とされる。制御信号802をHiにしてバイアストインバータ型光ディテクタ800を動作可能にすると、選択信号804a, 804b, 804cの何れかをHiにするかによって感度制御用素子による電流駆動能力が相違され、バイアスノード803に対するセンサ信号804の初期電位の差を所望に設定することが可能になる。選択信号804a, 804b, 804cは図示を省略するレジスタ値によって決定してよい。これにより、検出感度の修正もしくは最適化が容易になる。

【0085】

図12にICカード用の半導体集積回路としてICカード用マイクロコンピュータ（単にICカードマイコンとも記す）が例示される。ここでは、これまで述べてきた種々の光ディテクタを、どのようにICカードマイコンに適用するかについて示す。1100はICカードのICM（Integrated Circuit Module）例えばICカードマイコンである。1101は電源端子、1102はグラウンド端子、1103はクロック入力端子、1104と1105はI/O端子、1111は電源ブロック、1112はPLL（Phase-Locked Loop）ブロック、1113はCPUを含む論理回路ブロック、1114はインタフェースブロック、1115はSRAM、1116はROM、1117はEEPROM、1121は内部データバスである。

【0086】

ROM1116はCPUを含む論理回路ブロック1113中のCPUの制御プログラムを保有し、EEPROM1117は制御データ等を書換え可能に保有する。SRAM1115はCPUを含む論理回路ブロック1113中のCPUのワーク領域などに利用される。PLL1112はクロック入力端子1103から供給される外部クロックに基づいて内部クロックを生成する。

【0087】

一般にICカードの各外部端子には、高速性が要求されないため、ICカードマイコンは伝統的な5V電源のインタフェースを採用している。そのため、ICカードマイコン1100には電源は5Vが供給される。しかし、ディープサブミクロンプロセスより微細化が進んだICでは5Vの電源は高すぎるので、各回路に適切な電源電圧を供給するため降圧電源が必要となる。またEEPROM1117では、メモリの消去／書き込みのため5Vより高い電圧、グラウンドより低い電圧を必要とするため、それぞれチャージポンプ等を用いた昇圧電源／負電圧電源回路が必要となる。これらの電源回路をまとめたブロックが、電源ブロック1111である。電源ブロック1111は主にアナログ回路で構成される。このため、前記バイアストインバータ型光ディテクタ800、カレントミラー型光ディテクタ900、ディファレンシャルAMP型光ディテクタ1000等の回路が目立つこと無く組み込むことができる。目立つこと無くとは、アナログ回路故に、定電流を流す回路構成の光ディテクタが挿入されていても周りの回路構成に対して容易に識別し難い、という意味である。

【0088】

ICカードマイコン1100にはCPUを含む論理回路ブロック1113が内蔵されているため、PLLブロック1112が必要となる。PLLブロック1112はアナログ回路で構成されるため、前記バイアストインバータ型光ディテクタ800、カレントミラー型光ディテクタ900、ディファレンシャルAMP型光ディテクタ1000等が目立つこと無く組み込むことができる。

【0089】

CPUを含む論理回路ブロック1113やインタフェースブロック1114は、主としてデジタル回路で構成されるため、インバータ型光ディテクタ700を採用するのが適切である。適切であるとは、デジタル回路故に、プッシュ・プル構成の光ディテクタが挿入されていても周りの回路構成に対して容易に識別し難い、という意味である。

【0090】

SRAM1115、ROM1116、EEPROM1117は、メモリ素子であるためSRAM型光ディテクタ100、ダイオード追加SRAM型光ディテクタ500、電流リミッタ追加SRAM型光ディテクタ600等を採用するのが適切である。ここで適切とは、光ディテクタがメモリセル様の回路構成を備えるので周りのメモリセルに対して容易に識別し難い、という意味である。ROM1116やEEPROM1117はメモリセル構成がSRAMとは異なるためメモリアレイ中に混在させることは適切ではないが、メモリセルへ書き込むべきデータ若しくはメモリセルから読み出したデータを一時的に格納するバッファをSRAMメモリセル構成とし、その中にSRAM型光ディテクタを混在させればよい。

【0091】

各種光ディテクタによる光検出信号は、例えば論理和が採られ、論理信号はICカードマイコンのリセット信号（マスタリセット信号）の一つとされる。これにより、光を当ててリバースエンジニアリングのためのデータ収集を試みようとしても、その都度、ICカードマイコンにマスタリセットがかかって初期状態に戻され、リセットの解除は行われない。この結果、光照射によって不正なデータ収集を行おうとしても、ICカードの動作が停止し、統計的に暗号鍵等の解析を行うことを阻むことができる。

【0092】

このように、回路ブロックの特性に合わせて、適宜様々な種類の光ディテクタを組み込むことで、リバースエンジニアリングをより効果的に防ぐことができる。

【0093】

上記光ディテクタの組み込み法は様々な方法が考えられる。第1に、素子の配置によって出来た隙間に組み込む方法、第2に、格子状のパターンで組み込む方法などが良いと考えられる。

【0094】

図13には機能ブロックの素子配置の隙間に光ディテクタを組み込んだ様子が例示される。例えば一つの機能ブロック1604は、D型ラッチ回路のような第1基本セル1601、ナンドゲート（NAND）等の第2基本セル1602、インバータ等の第3基本セル1603が所要の機能を満足するように配置され、それによって生じた隙間に光ディテクタ1301が配置される。一般的にデジタル回路は基本セル1601、1602、1603等を並べることで、機能ブロック1604を構成する。基本セル1601～1603は配置を行い易いように、セル高さは統一されるが、セルによって幅は異なる。そのため機能ブロックを構成する時に、どうしても隙間が出来てしまう。一般的に、この隙間は何も配置しないか又はいわゆる隙間セルを配置するが、ここに光ディテクタ1301を組み込むことで、面積の増大なしに多数の機能ブロックに光ディテクタ1301を組み込むことができる。

【0095】

図14には格子状のパターンで光ディテクタを組み込んだ様子が例示される。特にリバースエンジニアリングを防ぎたい機能ブロック1704には、予め光ディテクタ1301を配置しておく。その配置はここでは格子状である。この手法では、光ディテクタ1301の隙間に基本セル1601～1603を配置するため、セルの隙間1701が多数発生するが、光ディテクタ1301の密度を調整できるので、リバースエンジニアリングの防止という点で優れる。

【0096】

図15にはD型フリップフロップに光検出回路を組み込んだ基本セルが例示される。リバースエンジニアリング防止を重要視するならば、論理回路の基本素子（フリップフロップ

プ、NAND、NOR、インバータ等)に、あらかじめ光ディテクタを組み込んでおき、それらを使用することで光ディテクタを高密度に配置することが容易になる。

【0097】

図15に例示される基本セル1501はD型フリップフロップの基本素子に対応され、D型フリップフロップ1502、光検出回路1301、及びワイヤード・オア結合素子1302から成る。この場合採用する光ディテクタは、動作時の消費電力がほぼゼロで、面積を小さく抑えることが出来る、インバータ型光ディテクタ700が最適であるので、光検出回路1301にインバータ型光ディテクタ700を採用する。ワイヤード・オア結合素子1302のドレインはその他の基本セルに設けられるワイヤード・オア結合素子のドレインに結合されればよい。

【0098】

図16には光ディテクタによる光検出の他に、電圧検出、周波数検出、配線切断検出機能を付加したICカードマイコンが例示される。図12に対して、電圧検出回路1201、周波数検出回路1202、配線切断検出回路1203、アクティブシールド配線(ラーメンパターン)1204が付加された点が相違される。

【0099】

電圧検出回路1201は電源ブロック1111で生成される内部動作電源の規定以下の降圧を検出する。プローブを介して内部電源ノードに異常な降圧電圧を印加して異常な動作をさせることによってリエンジニアリングの解析が行われること予想して、これを検出するために前記電圧検出回路1201を利用する。

【0100】

周波数検出回路1202はPLL1112で生成される内部クロックの周波数が規定の周波数以上にされたことを検出する。プローブを介して内部クロック供給ノードに異常な高周波を印加して異常な動作をさせることによってリエンジニアリングの解析が行われること予想して、これを検出するために前記周波数検出回路1202を利用する。

【0101】

配線切断検出回路1203はICカードマイコンの表面に配置されたアクティブシールド配線(ラーメンパターン)1204が切断されたことを検出する。アクティブシールド配線1204は図17に例示されるようにICカードマイコンの表面全体に緻密なパターンを描くように敷設される。ICカードマイコンの内部ノードにプローブを接触させるためにICカードマイコンの表面保護膜などを除去しようとすると一緒にアクティブシールド配線(ラーメンパターン)1204も切断され、これを検出しようとする。

【0102】

図18には光ディテクタによる光検出、電圧検出、周波数検出、及び配線切断検出により統合的にリセット信号を生成する回路構成が例示される。1301は種々の形態の光検出回路を総称する光検出回路、1302は光検出回路1301の検出信号を選択端子に受けるMOSトランジスタのようなワイヤード・オア素子、1308は電圧検出回路1201からの検出信号を選択端子に受けるMOSトランジスタのようなワイヤード・オア素子、1309は周波数検出回路1202からの検出信号を選択端子に受けるMOSトランジスタのようなワイヤード・オア素子である。1303はリセット回路、1304はリセット信号、1305はプルダウン抵抗、1306はプルアップ抵抗、1204はアクティブシールド配線である。前記ワイヤード・オア素子1301、1308、1309、プルアップ抵抗1306、プルダウン抵抗1305、及びアクティブシールド配線1204は配線1307に共通接続される。

【0103】

前記プルアップ抵抗1306の方が、プルダウン抵抗1305より抵抗値が小さいため、配線1307の電位は、電源電圧付VDD近となる光検出回路1301のどれかが光の入射を検出するとワイヤード・オア素子1302がオン状態にされ、電圧検出回路1201が内部電圧の異常を検出するとワイヤード・オア素子1308がオン状態にされ、周波数検出回路1202が周波数の異常を検出するとワイヤード・オア素子1309がオン状

態にされる。何れかのワイヤード・オア素子がオン状態にされると、配線 1307 の電位はグラウンド VSS 付近まで降下する。これをリセット回路 1303 が検出し、リセット信号 1304 をアサートして IC カードマイコンを初期化する。配線 1307 を切断しても、或はアクティブシールド配線 1204 を切断しても、プルダウン抵抗 1305 の効果で、配線 1307 の電位はグラウンド VSS 付近まで降下し、同様に IC カードマイコンは初期化される。リセット指示の解除は行われず、IC カードの動作は停止する。

【0104】

また、図 2 に示す光ディテクタ素子を構成する MOS の上層で、遮光をするための金属箔を形成する場合、アクティブシールド配線やその他の配線により形成するようにしてもよい。この場合 MOS の大きさに対して配線の幅は狭いのが通常であるため、遮光する MOS の上層の配線を密にし、遮光しない MOS の上層の配線を疎にすることにより、光の強度に差がつくようにしてもよい。

【0105】

図 19 には接触インタフェース形式の IC カード 1130 の外観が例示される。合成樹脂から成るカード基板 1131 には、特に制限されないが、外部インタフェース部として、電極パターンによって形成された外部端子 1132 が表面に露出され、前記図 12 及び図 16 に例示される IC カードマイコン 1100 が埋め込まれている。前記電極パターンには IC カードマイコン 1100 の対応する外部端子が結合される。

【0106】

図 20 には非接触インタフェース形式の IC カード 1134 の外観が例示される。合成樹脂から成るカード基板 1135 には、特に制限されないが、外部インタフェース部としてアンテナ 1136 が埋め込まれ、前記図 12 及び図 16 に例示される IC カードマイコン 1100 が埋め込まれる。この例では、IC カードマイコン 1100 はインタフェースブロック 1114 に高周波部を有し、この高周波部に前記アンテナ 1136 が結合される。

【0107】

前記 IC カード 1130、1134 を例えば電子マネーシステムで利用するとき、前記 EEPROM 1117 には暗号鍵や金額情報などが暗号化されて格納され、電子マネーを利用するとき暗号鍵や金額情報が復号され、復号された情報を用いて正当な利用か否かが判定され、必要な金額が銀行に送金され、或いは別の IC カードに所要の金額が転送される。

【0108】

また、前記 IC カード 1130、1134 が携帯電話機に装着されて使用されるとき、前記 EEPROM 1117 には使用者の電話番号、ID 番号、課金情報等が暗号化されて格納され、電話を利用するときそれら情報が復号され、復号された情報を用いて正当な利用か否かが判定され、使用度数に応じて課金情報が更新され、再度暗号化される。

【0109】

上記 IC カード 1130、1134 によれば、前記 IC カードマイコン 1100 光検出による強制リセット作用により、暗号鍵などのデータハッキングが防御され、利用者の損害発生を抑制することができる。

【0110】

図 21 には図 7 のインバータ型光ディテクタ 700 の変形例に係る光ディテクタ 700A が示される。図 7 の回路では受光素子として光検出 MOS トランジスタ 712 におけるドレインの PN 接合を利用している。光ディテクタ 700A では、それをダイオード 1812 の PN 接合に置き換えている。逆バイアスされたダイオード 1812 に光が照射された場合にも、ドレインと同様漏れ電流が発生する。

【0111】

負論理イネーブル信号 701 が Hi に立ち下がると、出力の電位 703 が電源電位 VDD まで上昇する。その時ディテクタ出力信号 702 の電位はグラウンド電位 VSS となる。ダイオード 1812 に光が照射されると漏れ電流が発生し、光の強度が十分大きく漏れ

電流の大きさが感度調整MOSトランジスタ711の電流駆動力より大きくなった時、センサ出力信号703は下降し、出力インバータ713の論理スレッシュホールドを下回り、ディテクタ出力702がHiに立ち上がる。

【0112】

図22には図7のインバータ型光ディテクタ700の別の変形例に係る光ディテクタ700Bが示される。感度調整用MOSトランジスタ1911をPチャンネル型で構成し、光検出用MOSトランジスタをNチャンネル型で構成した点が相違される。

【0113】

正論理イネーブル信号1901がHiに立ち上がると、電位1903がグラウンド電位VSSまで下降する。その時ディテクタ出力信号1902の電位はグラウンド電位VSSとなる。オフ状態のMOSトランジスタ1911のドレインに光が照射されると漏れ電流が発生し、光の強度が十分大きく漏れ電流の大きさがMOSトランジスタ1912の電流駆動力より大きくなった時、電位1903は上昇し、バッファ1913の論理スレッシュホールドを上回り、ディテクタ出力信号1902がHiに立ち上がる。

【0114】

図23には図22の変形例に係る光ディテクタ700Cが示される。図22で受光素子に使用されているMOSトランジスタ1911をダイオード2011に置き換えている。ダイオード2011による基本的な動作形態は図21で説明したのと同様であるからその詳細な動作説明については省略する。

【0115】

図24には図8のバイアストインバータ型光ディテクタ800の変形例に係る光ディテクタ800Bが示される。図8の回路では受光素子として光検出MOSトランジスタ817におけるドレインのPN接合を利用している。図24ではMOSトランジスタ817の代わりに、ダイオード2110を受光素子として利用する。ダイオード2110は出力804と回路の接地電位VSSとの間に逆バイアス状態で接続される。

【0116】

MOSトランジスタ813とMOSトランジスタ817の電流駆動力が、MOSトランジスタ813>MOSトランジスタ817、と設定されているので、センサ信号804の電位は、MOSトランジスタ819～822で構成されるインバータの論理スレッシュホールドより高い。ここで、ダイオード2110に光が照射されると漏れ電流が発生し、光の強度が十分大きく漏れ電流が十分大きい場合、センサ信号804の電位が、MOSトランジスタ819～822で構成されるインバータの論理スレッシュホールドより低くなる。これによりディテクタ出力805がグラウンド電位付近から電源電位VDD付近まで立ち上がり、光の照射を検出できる。

【0117】

図25には図24の変形例に係る光ディテクタ800Cが示される。図22で追加したダイオード2110をMOSトランジスタ817のソースと回路の接地電位VSSとの間に配置した点で相違する。基本的な動作形態は図24で説明したのと同様であるからその詳細な動作説明は省略する。

【0118】

図26には図8のバイアストインバータ型光ディテクタ800の変形例に係る光ディテクタ800Dが示される。ここでは、pチャンネル型MOSトランジスタ2216とnチャンネル型MOSトランジスタ2217によって構成されるインバータの当該MOSトランジスタ2216を光検出用MOSトランジスタとし、プルアップ用のMOSトランジスタ823に代えてセンサ出力804をプルダウンするMOSトランジスタ2223を採用する。

【0119】

図8では、MOSトランジスタの電流駆動力は、MOSトランジスタ812=MOSトランジスタ816、MOSトランジスタ813>MOSトランジスタ817に設定されていたが、図26の回路では、MOSトランジスタ812>MOSトランジスタ2216、

MOSトランジスタ813=MOSトランジスタ2217と設定される。よって、センサ信号804の電位は、MOSトランジスタ819~822で構成されるインバータの論理スレッシュホールドより低い。ここで受光素子として使用されるMOSトランジスタ2216に光が照射されると漏れ電流が発生し、光の強度が十分大きく漏れ電流が十分大きい場合、センサ信号804の電位が、MOSトランジスタ819~822で構成されるインバータの論理スレッシュホールドより高くなる。これによりディテクタ出力信号2201がグラウンド電位VSS付近から電源電位VDD付近まで立ち上がり、これによって光の照射が検出される。

【0120】

図27には図26の変形例に係る光ディテクタ800Eが示される。ここでは、受光素子に使用されていたMOSトランジスタ2216の代わりに、受光素子としてダイオード2310を加えた。動作については省略する。図示はしないが、ダイオード2310の接続は、図25と同様に、MOSトランジスタ2216のソースと電源電圧VDDの間に逆バイアスで接続する形態に変更可能である。

【0121】

図28には図9のカレントミラー型光ディテクタ900の変形例に係る光ディテクタ900Aが示される。図9の回路で受光素子として使用されているMOSトランジスタ919の代わりに、ダイオード2410を受光素子として追加した点が相違される。ダイオード2410は逆バイアス状態（逆方向接続状態）でMOSトランジスタ916に並列接続される。

【0122】

MOSトランジスタ916とMOSトランジスタ919の電流駆動力は、MOSトランジスタ916>MOSトランジスタ919と設定されているので、センサ信号904の電位は、MOSトランジスタ920~923で構成されるインバータの論理スレッシュホールドより高い。ここで、ダイオード2410に光が照射されると漏れ電流が発生し、光の強度が十分大きく漏れ電流が十分大きい場合、センサ信号904の電位が、MOSトランジスタ920~923で構成されるインバータの論理スレッシュホールドより低くなる。これによりディテクタ出力905がグラウンド電位VSS付近から電源電位VDD付近まで立ち上がり、光の照射が検出される。

【0123】

図29には図9のカレントミラー型光ディテクタ900の変形例に係る光ディテクタ900Bが示される。図9に対してMOSトランジスタの導電型（p型、n型）を入れ替えて構成した点が相違される。図9の回路ではMOSトランジスタ916、919の電流駆動力には、MOSトランジスタ916>MOSトランジスタ919の関係が設定されていたが、図29の回路でも同様に、MOSトランジスタ2516>MOSトランジスタ2519の関係が設定される。よって、センサ信号2504の電位は、MOSトランジスタ2520~2523で構成されるインバータの論理スレッシュホールドより低い。ここで受光素子として使用されるMOSトランジスタ519に光が照射されると漏れ電流が発生し、光の強度が十分大きく漏れ電流が十分大きい場合、センサ信号2504の電位が、MOSトランジスタ2520~2523で構成されるインバータの論理スレッシュホールドより高くなる。これによりディテクタ出力2506がグラウンド電位VSS付近から電源電位VDD付近まで立ち上がり、光の照射が検出される。

【0124】

図30には図29のカレントミラー型光ディテクタ900Bの変形例に係る光ディテクタ900Cが示される。図29の回路で受光素子に使用されているMOSトランジスタ2519の代わりに、受光素子としてダイオード2610を追加した点が相違される。ダイオード2610は逆バイアス状態（逆方向接続状態）でMOSトランジスタ2516に並列接続される。基本的な動作形態は図28で説明したのと同様であるからその詳細な動作説明は省略する。

【0125】

図31には図10のディファレンシャルAMP型光ディテクタ1000の変形例に係る光ディテクタ1000Aが示される。同図に示される光ディテクタ1000Aには、図10において受光素子として使用しているMOSトランジスタ1019の代わりに、ダイオード2710を受光素子として追加した。MOSトランジスタ1016とMOSトランジスタ1019の電流駆動力は、MOSトランジスタ1016>MOSトランジスタ1019と設定されているので、センサ信号1004の電位は、MOSトランジスタ1020～1023で構成されるインバータの論理スレッシュホールドより高い。ここで、ダイオード2710に光が照射されると漏れ電流が発生し、光の強度が十分大きく漏れ電流が十分大きい場合、センサ信号1004の電位が、MOSトランジスタ1020～1023で構成されるインバータの論理スレッシュホールドより低くなる。これによりディテクタ出力1005がグラウンド電位VSS付近から電源電位VDD付近まで立ち上がり、光の照射が検出される。

【0126】

図32には図10のディファレンシャルAMP型光ディテクタ1000Aの変形例に係る光ディテクタ1000Bが示される。図31に対してMOSトランジスタの導電型（p型、n型）を入れ替えて構成した点が相違される。図10の回路では電流供給能力がMOS1016トランジスタ>MOSトランジスタ1019と設定されていたが、図32の回路でも同様に、電流駆動能力はMOSトランジスタ2816>MOSトランジスタ2819と設定されている。よって、センサ信号2804の電位は、MOSトランジスタ2820～2823で構成されるインバータの論理スレッシュホールドより低い。ここで受光素子として使用されるMOSトランジスタ2819に光が照射されると漏れ電流が発生し、光の強度が十分大きく漏れ電流が十分大きい場合、センサ信号2804の電位が、MOSトランジスタ2820～2823で構成されるインバータの論理スレッシュホールドより高くなる。これによりディテクタ出力2806がグラウンド電位VSS付近から電源電位VDD付近まで立ち上がり、光の照射が検出される。

【0127】

図33には図32のディテクタ1000Bの変形例に係る光ディテクタ1000Cが示される。図29の回路で受光素子に使用されているMOSトランジスタ2819の代わりに、受光素子としてダイオード2910を追加した点が相違される。ダイオード2910は逆バイアス状態（逆方向接続状態）でMOSトランジスタ2819に並列接続される。基本的な動作形態は図29で説明したのと同様であるからその詳細な動作説明は省略する。

【0128】

図34には図29の光ディテクタの変形例に係る光ディテクタ900Dが示される。図29のように受光素子が独立している場合、ダイオードを他から離して配置することが可能である。その場合、図34に例示されるように、受光素子として複数のダイオード2610__1～2610__3を持つことが可能である。受光素子部分としてのダイオードのみが複数存在しても、その他の回路部分である光ディテクタ本体900corは単体で済むため、回路面積が小さく、消費電力が少なく済む。受光素子としてのダイオード2610__1～2610__3のうち1つでも光が照射されれば、これに反応して光検出される。

【0129】

また、光ディテクタ本体900corが正しく動作するかをテストするために、テスト回路3010を図のように接続するとよい。テスト回路3010が電流を掃き出す事で、擬似的にセンサが反応した状態を作り出すことができ、光ディテクタ本体が動作するかどうかをテストすることができる。尚、図21、図23、図24、図27、図28、図31及び図33の各回路も同様の構成で、複数のダイオードと一つの光ディテクタ本体という構成を採用することが可能である。

【0130】

図35には受光素子として使用するダイオードのデバイス断面構成が例示される。ダイ

オードという素子は p 型半導体と n 型半導体が接合すれば、どこにでも構成することができる。例えば p 型基板 3110 と電源分離用 n 型拡散層 3120 の PN 接合がダイオードとして使用できる。他にも (1) 電源分離用 n 型拡散層 3120 と p 型ウェル領域 (p-WELL) 3130、(2) p-WELL 3130 と N⁺ 拡散層 3140、(3) n-WELL 3150 と P⁺ 拡散層 3160、等がダイオードとして使用可能である。このようにダイオードとは pn 接合のことであり、他の素子の一部であっても、それはダイオードという概念で把握することができる。さらに、キャパシタや抵抗のようにシリコン基板に形成されない素子の直下の拡散層を利用してダイオードを構成することにより、ダイオードの追加による面積増加を抑えることができる。

【0131】

以上本発明者によってなされた発明を実施形態に基づいて具体的に説明したが、本発明はそれに限定されるものではなく、その要旨を逸脱しない範囲において種々変更可能であることは言うまでもない。

【0132】

例えば、スタティックラッチを主体とする光ディテクタは SRAM 以外のメモリのメモリアレイに配置することも可能である。IC カードマイコンに設けられる回路モジュールは図 12 などで説明した内容に限定されず、タイマカウンタ等その他の回路モジュールを搭載してもよい。本発明は IC カードマイコン以外のシステムオンチップに係る別の半導体集積回路にも広く適用することができる。尚、上記金属による遮光とドレイン面積の増大という技術的手段は本発明における光ディテクタ以外の一般的な光検出用の光ディテクタにも適用可能である。

【図面の簡単な説明】

【0133】

【図 1】本発明の第 1 実形態である SRAM 型光ディテクタを例示する回路図である。

【図 2】SRAM 型光ディテクタの光検出素子以外を金属皮膜で遮光するパターンの例を示す説明図である。

【図 3】オフ状態の MOS トランジスタへ光子が入射した場合の動作を示す説明図である。

【図 4】SRAM 型光ディテクタの SRAM への組み込み状と共に SRAM モジュールの全体的な構成を示すブロック図である。

【図 5】ダイオード追加 SRAM 型光ディテクタを示す回路図である。

【図 6】電流リミッタ追加 SRAM 型光ディテクタを示す回路図である。

【図 7】インバータ型光ディテクタを示す回路図である。

【図 8】バイアストインバータ型光ディテクタを示す回路図である。

【図 9】カレントミラー型光ディテクタを示す回路図である。

【図 10】ディファレンシャル AMP 型光ディテクタを示す回路図である。

【図 11】図 8 のバイアストインバータ型光ディテクタ 800 の変形例を示す回路図である。

【図 12】各種光ディテクタを組み込んだ様子を示す IC カードマイコンの概略構成を示すブロック図である。

【図 13】機能ブロックの素子配置の隙間に光ディテクタを組み込んだ様子为例示するレイアウト説明図である。

【図 14】機能ブロックに格子状のパターンで光ディテクタを組み込んだ様子为例示するレイアウト説明図である。

【図 15】D 型フリップフロップに光ディテクタを組み込んだ基本セルを例示する回路図である。

【図 16】光ディテクタによる光検出の他に、電圧検出、周波数検出、配線切断検出機能を付加した IC カードマイコンを全体的に示すブロック図である。

【図 17】IC カードマイコンの表面全体に緻密なパターンとしてアクティブシール

ド配線を敷設した様子を示す説明図である。

【図18】光ディテクタによる光検出、電圧検出、周波数検出、及び配線切断検出により統合的にリセット信号を生成する回路構成を例示する説明図である。

【図19】接触インタフェース形式のICカードの外観を例示する平面図である。

【図20】非接触インタフェース形式のICカードの外観を例示する平面図である。

【図21】図7のインバータ型光ディテクタの変形例に係る光ディテクタを示す回路図である。

【図22】図7のインバータ型光ディテクタの別の変形例に係る光ディテクタを示す回路図である。

【図23】図22の変形例に係る光ディテクタを示す回路図である。

【図24】図8のバイアストインバータ型光ディテクタの変形例に係る光ディテクタを示す回路図である。

【図25】図24の変形例に係る光ディテクタを示す回路図である。

【図26】図8のバイアストインバータ型光ディテクタの変形例に係る光ディテクタを示す回路図である。

【図27】図26の変形例に係る光ディテクタを示す回路図である。

【図28】図9のカレントミラー型光ディテクタの変形例に係る光ディテクタを示す回路図である。

【図29】図9のカレントミラー型光ディテクタの別の変形例に係る光ディテクタを示す回路図である。

【図30】図29のカレントミラー型光ディテクタの変形例に係る光ディテクタを示す回路図である。

【図31】図10のディファレンシャルAMP型光ディテクタの変形例に係る光ディテクタを示す回路図である。

【図32】図10のディファレンシャルAMP型光ディテクタの別の変形例に係る光ディテクタを示す回路図である。

【図33】図32のディテクタの変形例に係る光ディテクタを示す回路図である。

【図34】図29の光ディテクタの変形例に係る光ディテクタを示す回路図である。

【図35】受光素子として使用するダイオードのデバイス構造を説明するための断面図である。

【符号の説明】

【0134】

100 SRAM型光ディテクタ

111、112、113、114 スタティックラッチを構成するMOSトランジスタ

120 スタティックラッチ

302 ドレイン拡散領域

303 ソース拡散領域

311 ドレイン端子

312 ゲート端子

313 ソース端子

314 接地端子

320 光子

400 SRAMブロック

401 メモリセルアレイ

402 冗長セルアレイ

403 冗長プログラム回路

407 ECC回路

511、512 ダイオード

611、612 電流リミッタMOSトランジスタ

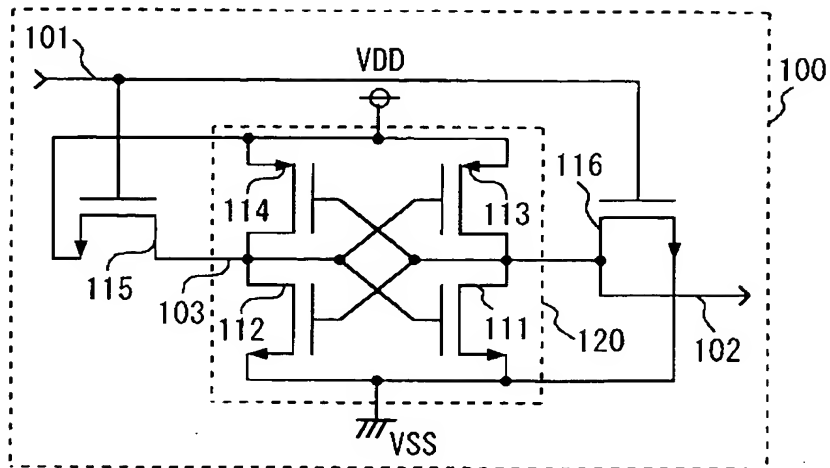
700、700A、700B、700C インバータ型光ディテクタ

711 感度調整MOSトランジスタ
712 光検出MOSトランジスタ
800、800A、800B、800C、800D、800E バイアストインバータ
型光ディテクタ
813、821 感度制御MOSトランジスタ
817 光検出MOSトランジスタ感度制御MOSトランジスタ
813a、813b、813c 感度制御MOSトランジスタ
900、900A、900B、900C、900D カレントミラー型光ディテクタ
916 感度調整MOSトランジスタ
919 光検出MOSトランジスタ
1000、1000A、1000B、1000C デイファレンシャルAMP型光ディ
テクタ
1016 感度調整MOSトランジスタ
1019 光検出MOSトランジスタ
1100 ICカードマイコン
1111 電源ブロック
1112 PLLブロック
1113 CPUを含む論理回路ブロック
1114 インタフェースブロック
1115 SRAM
1116 ROM
1117 EEPROM
1130 ICカード
1131、1135 カード基板
1132 外部端子
1136 アンテナ
1201 電圧検出回路
1202 周波数検出回路
1203 配線切断検出回路
1204 アクティブシールド配線
1301 光検出素子
1302 ワイヤード・オア結合素子
1303 リセット回路
1304 リセット信号
1305 プルダウン抵抗
1306 プルアップ抵抗
1307 配線
1308、1309 ワイヤード・オア結合素子
1501 基本セル
1502 D型フリップフロップ
1812、2011、2110、2310、2410、2610、2610__1~26
10__3、2710、2910 ダイオード

【書類名】 図面

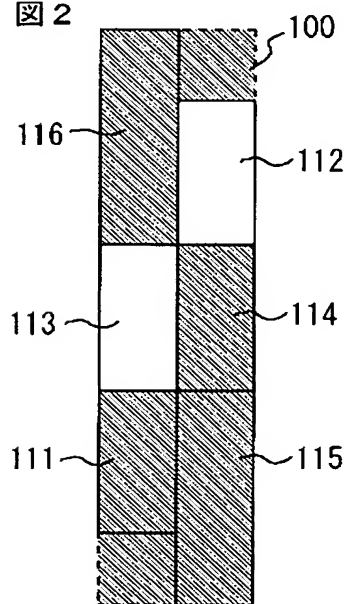
【図 1】

図 1



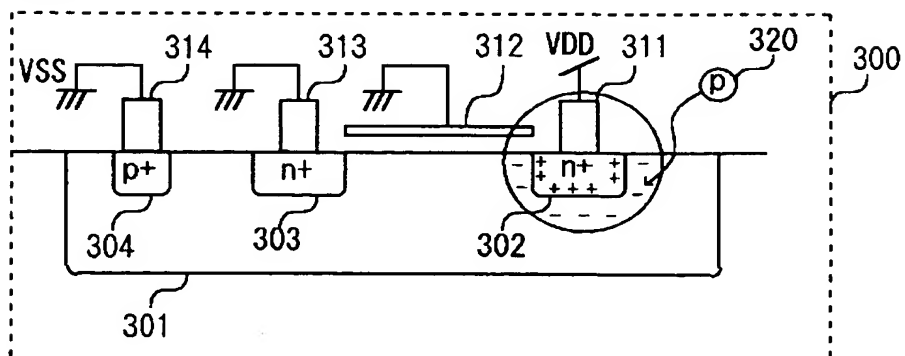
【図 2】

図 2

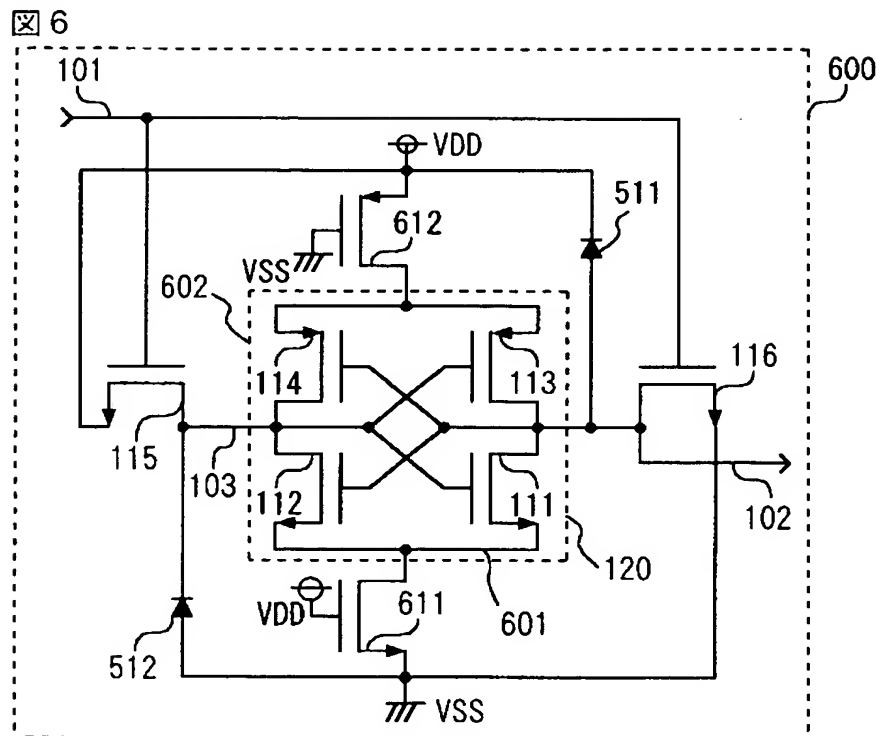


【図 3】

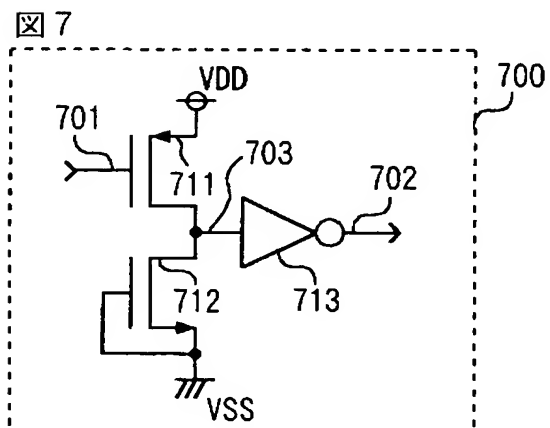
図 3



【図 6】

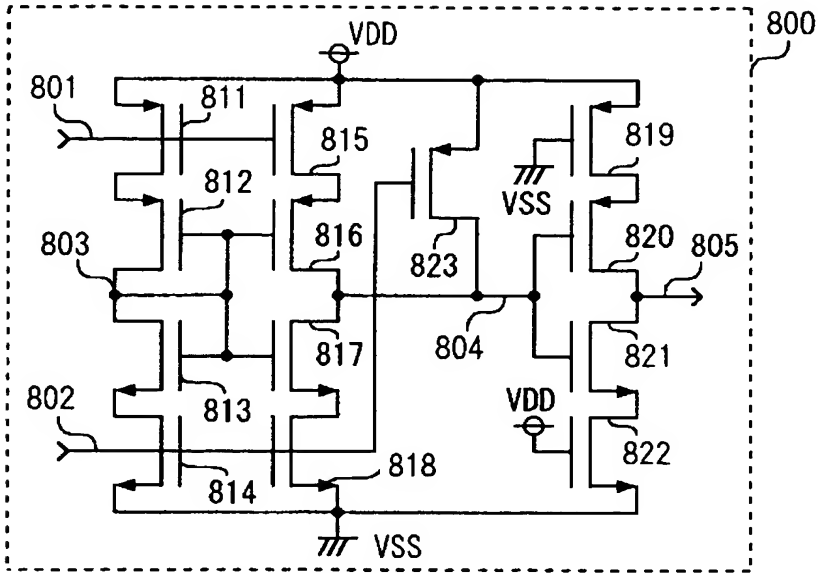


【図 7】



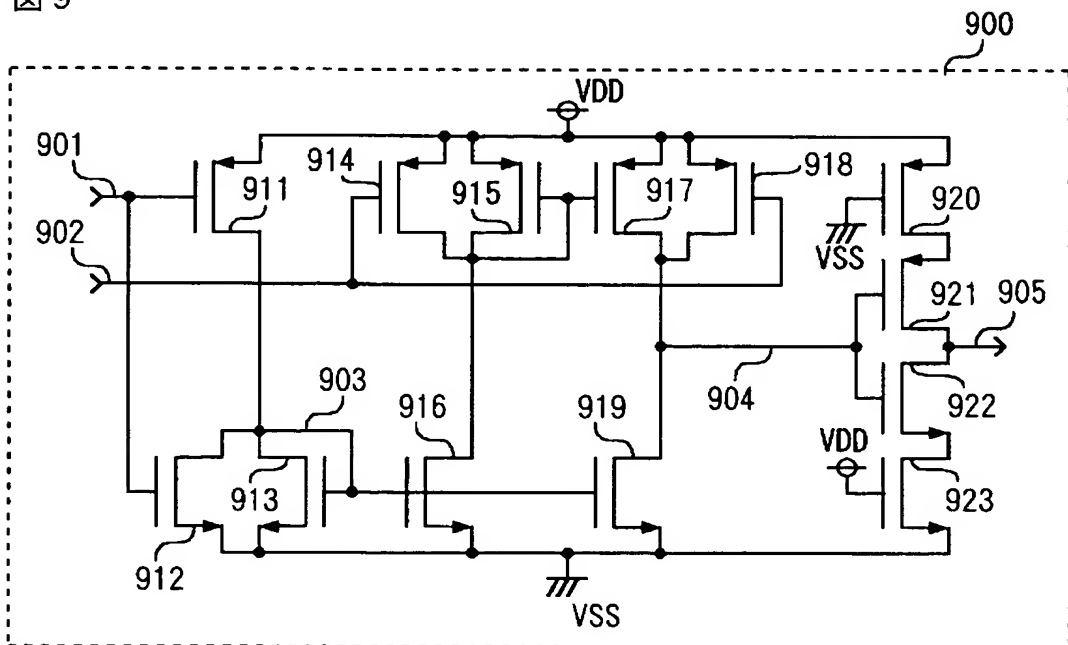
【図 8】

図 8



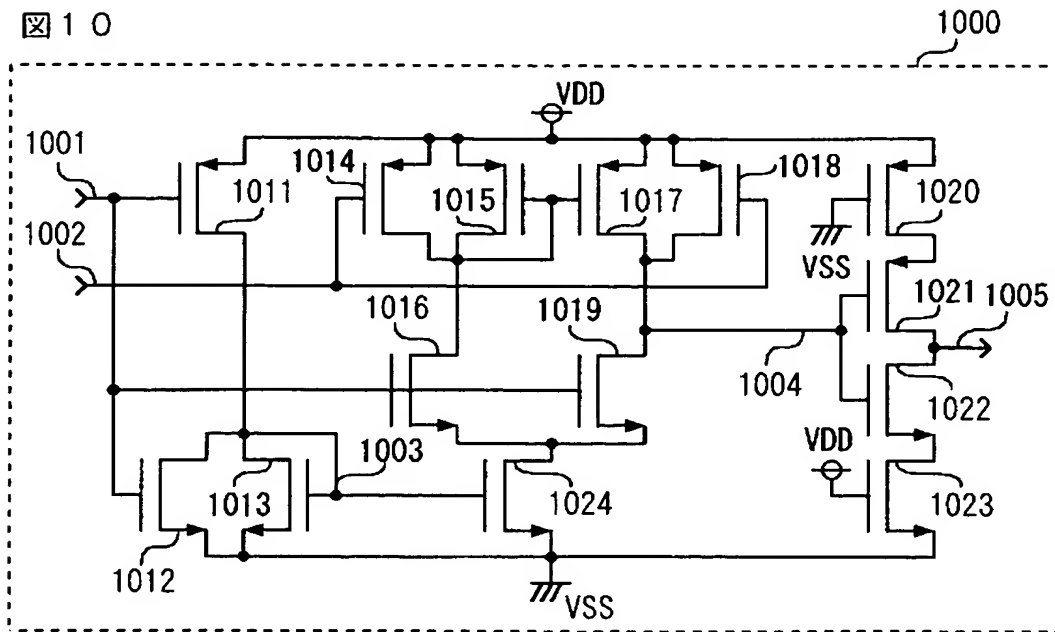
【図 9】

図 9



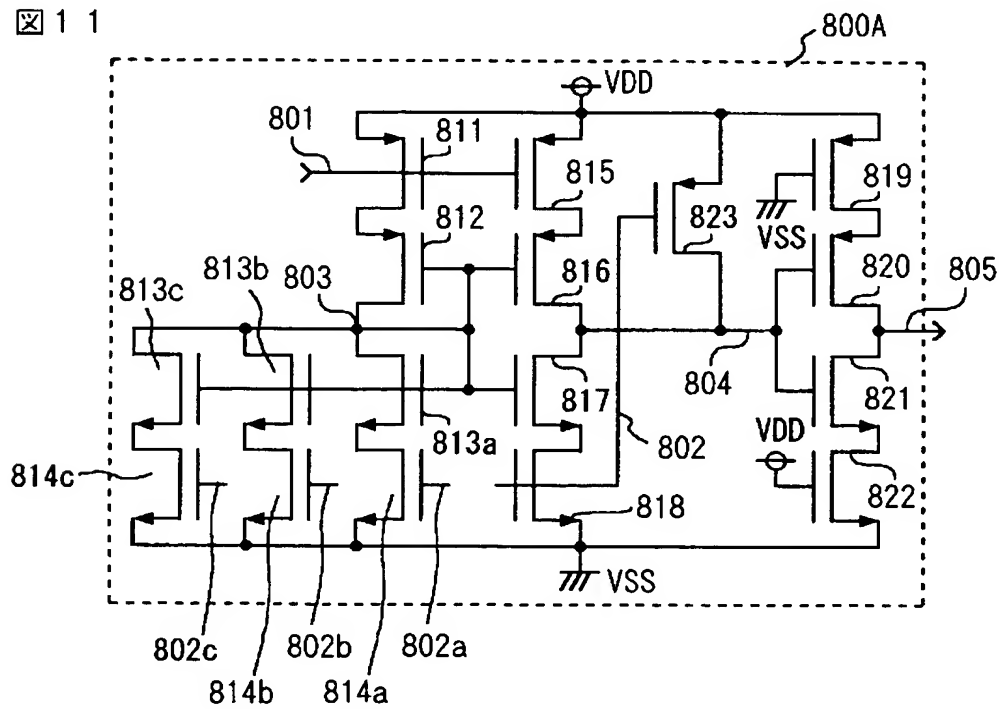
【図 10】

図 10



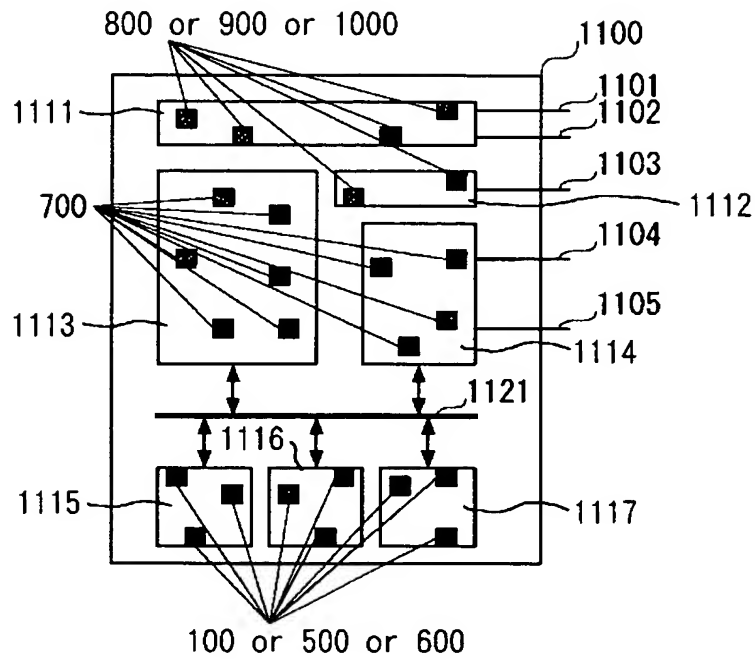
【図 11】

図 11



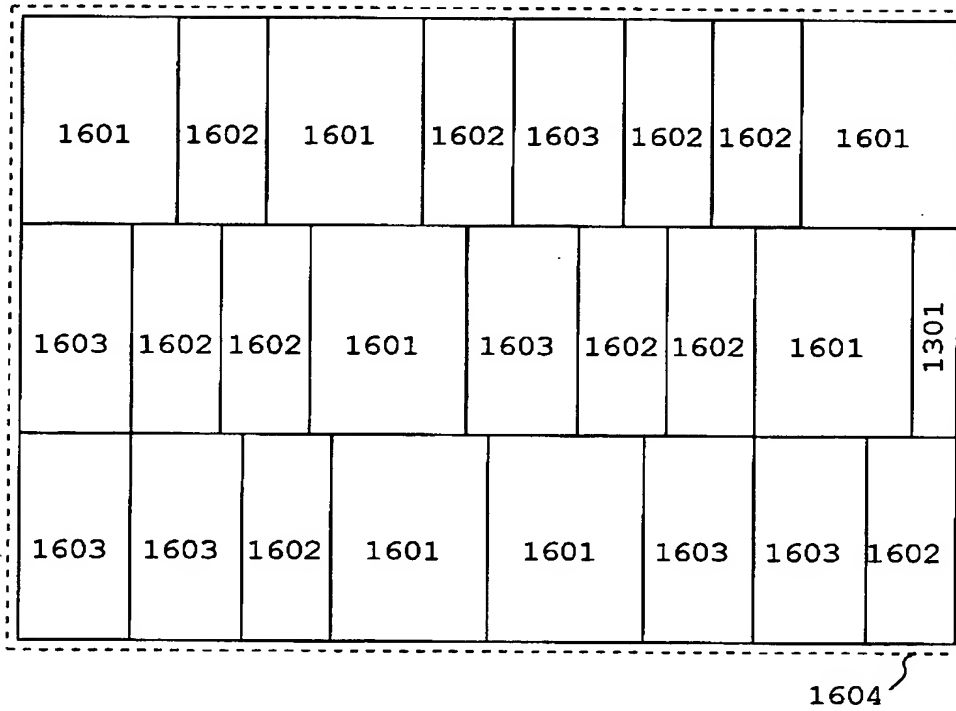
【図 12】

図 12



【図 13】

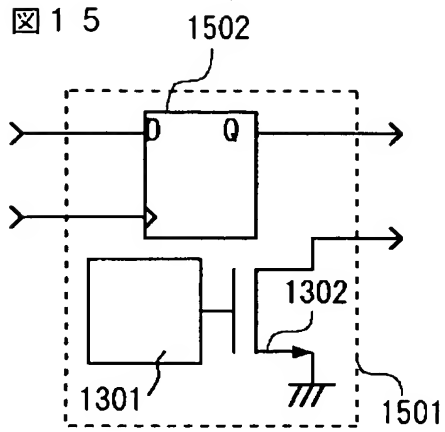
図 13



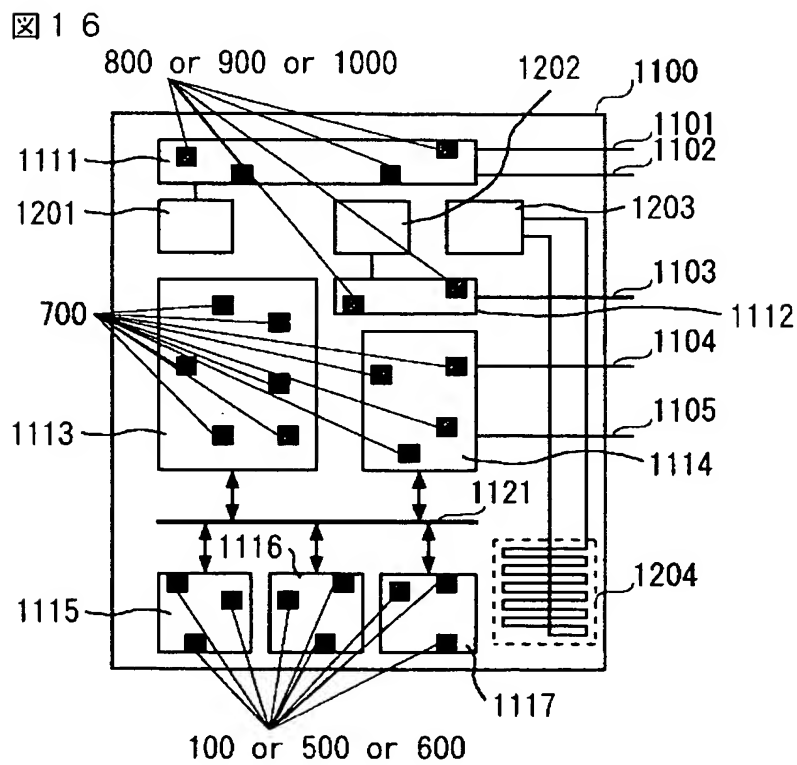
【図 14】

[illegible]

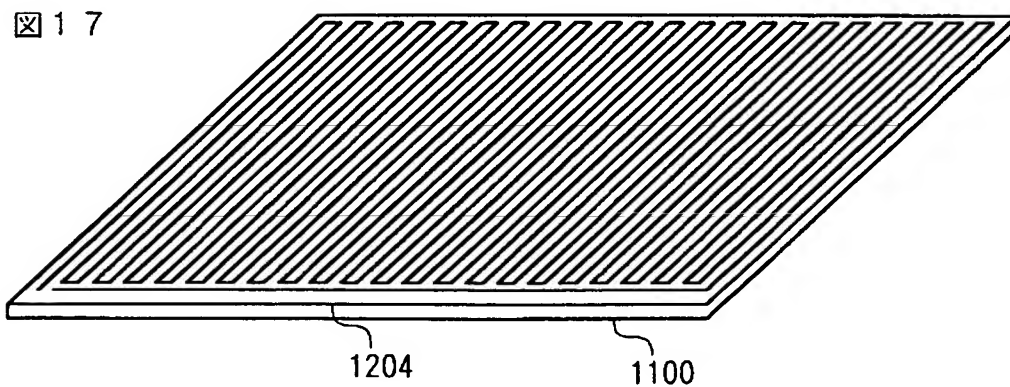
【図 15】



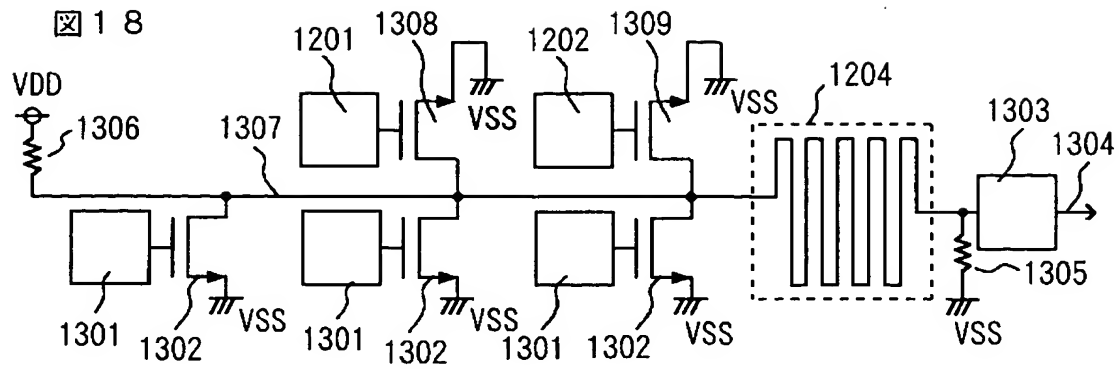
【図 16】



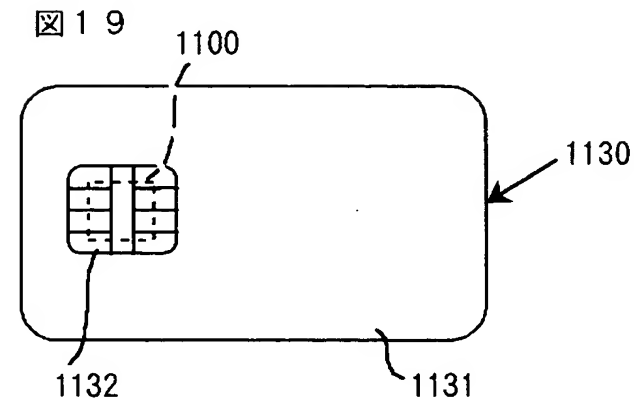
【図 17】



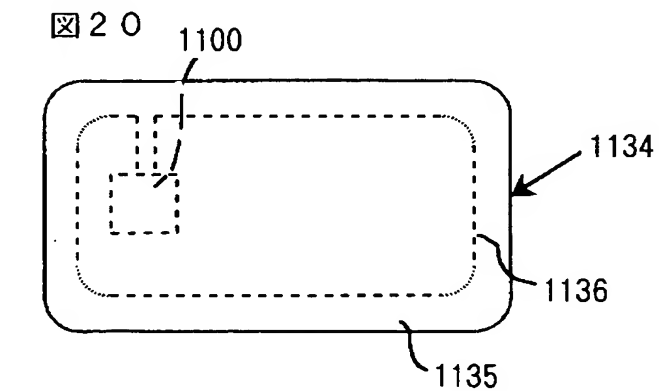
【図 18】



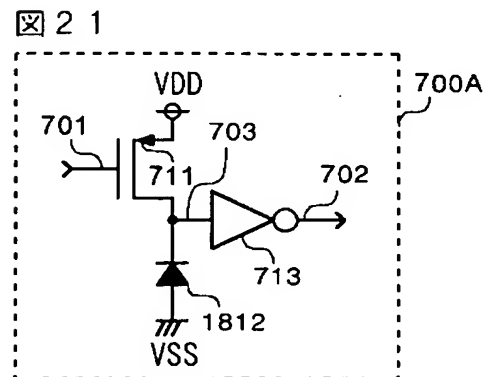
【図 19】



【図 20】

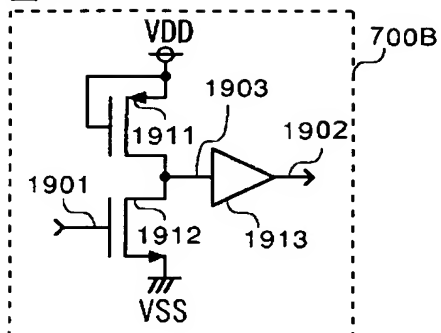


【図 21】



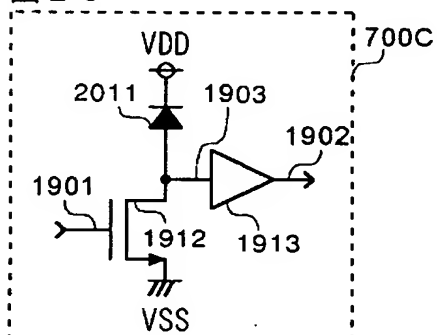
【図 2 2】

図 2 2



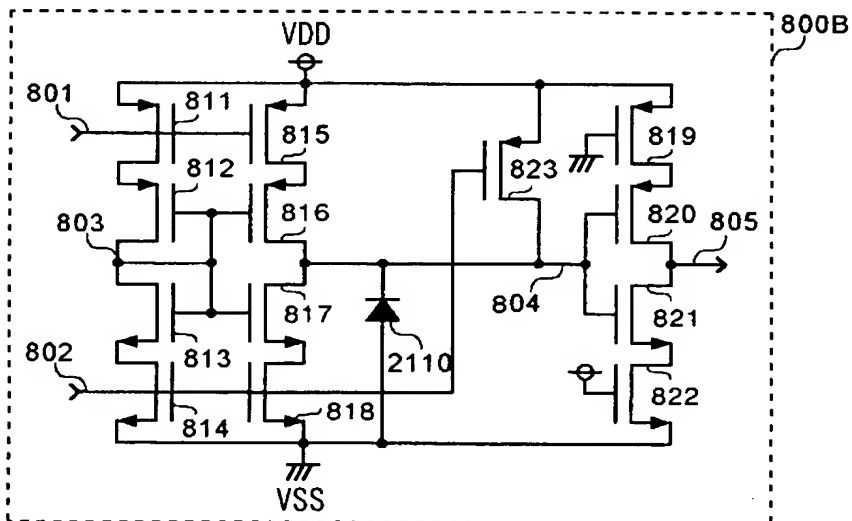
【図 2 3】

図 2 3



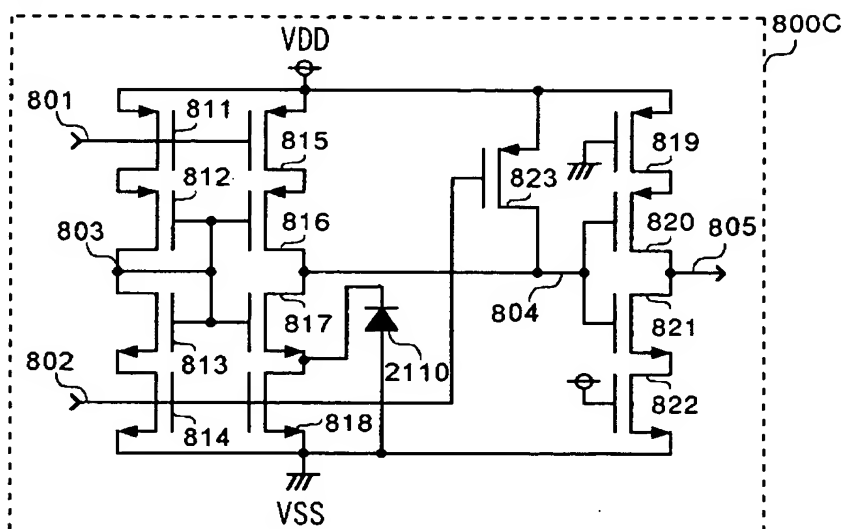
【図 2 4】

図 2 4



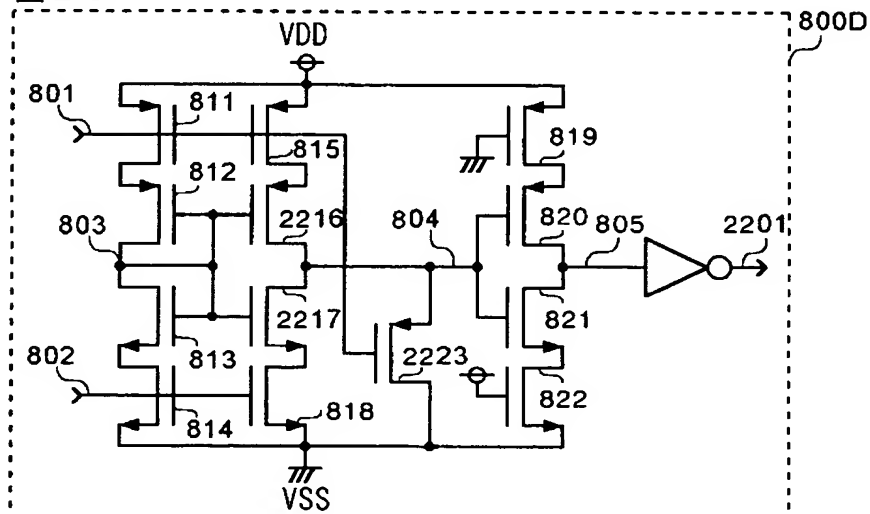
【図 25】

図 25



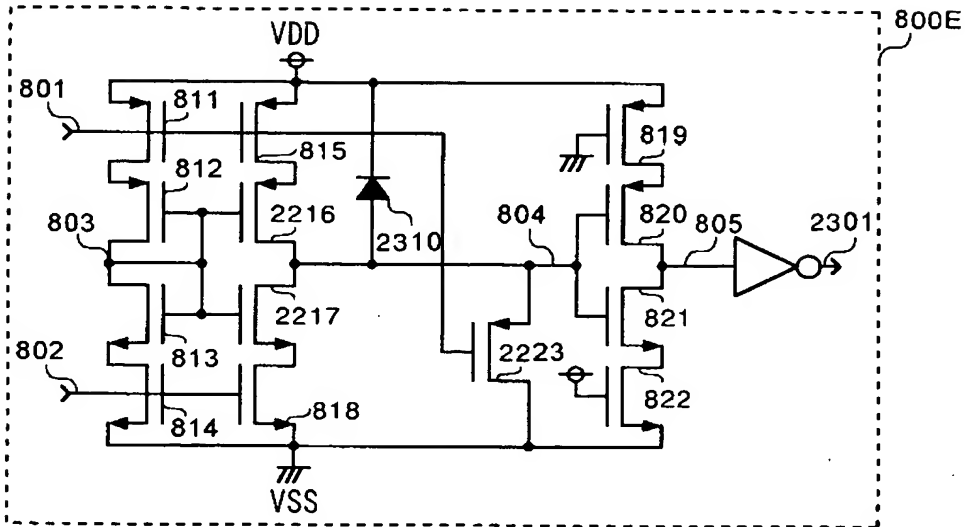
【図 26】

図 26



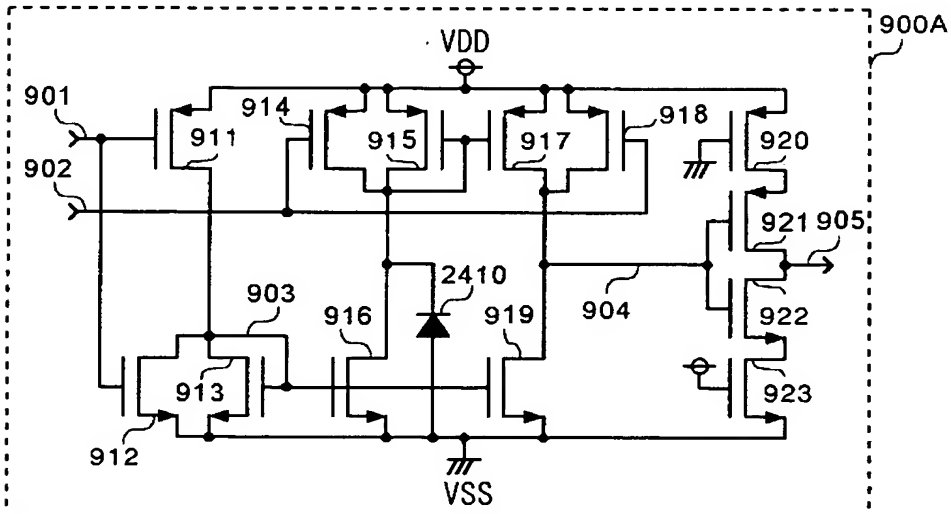
【図 27】

図 27



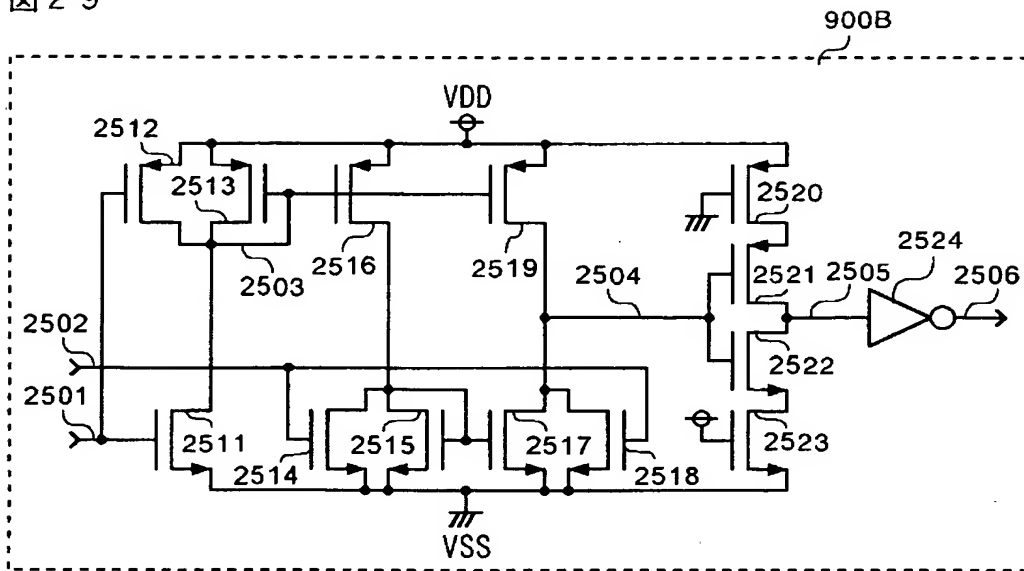
【図 28】

図 28



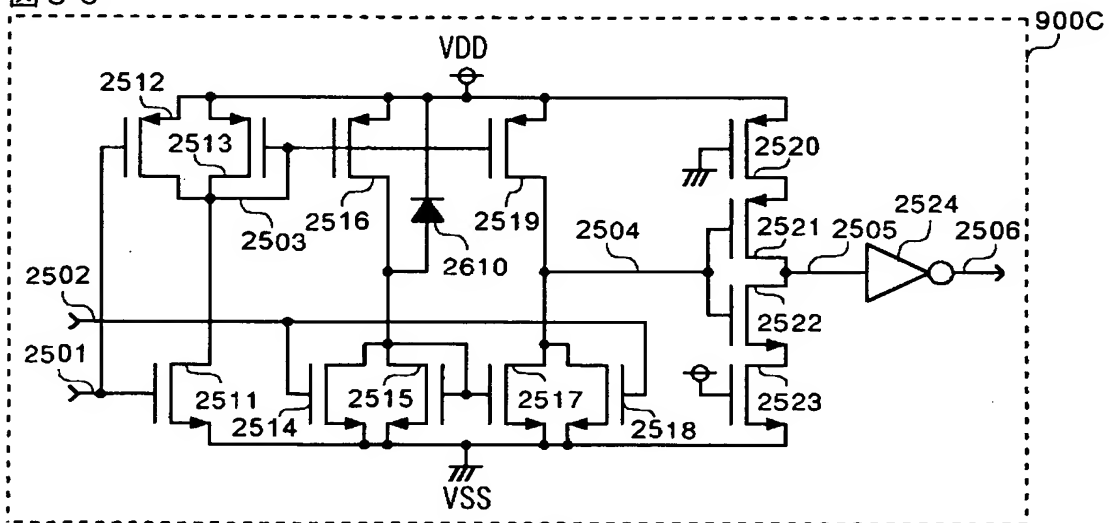
【図 29】

図 29



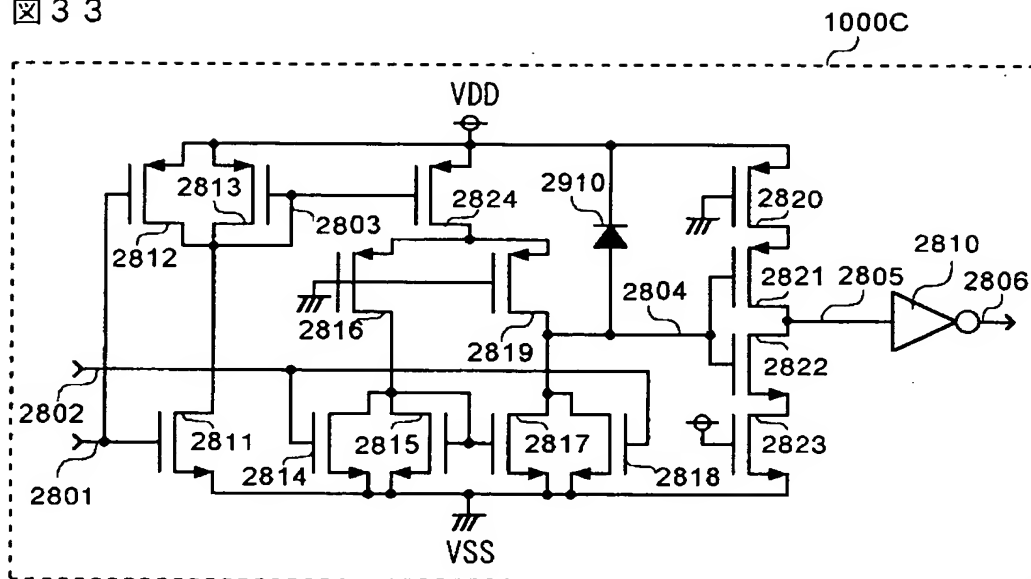
【図 30】

図 30



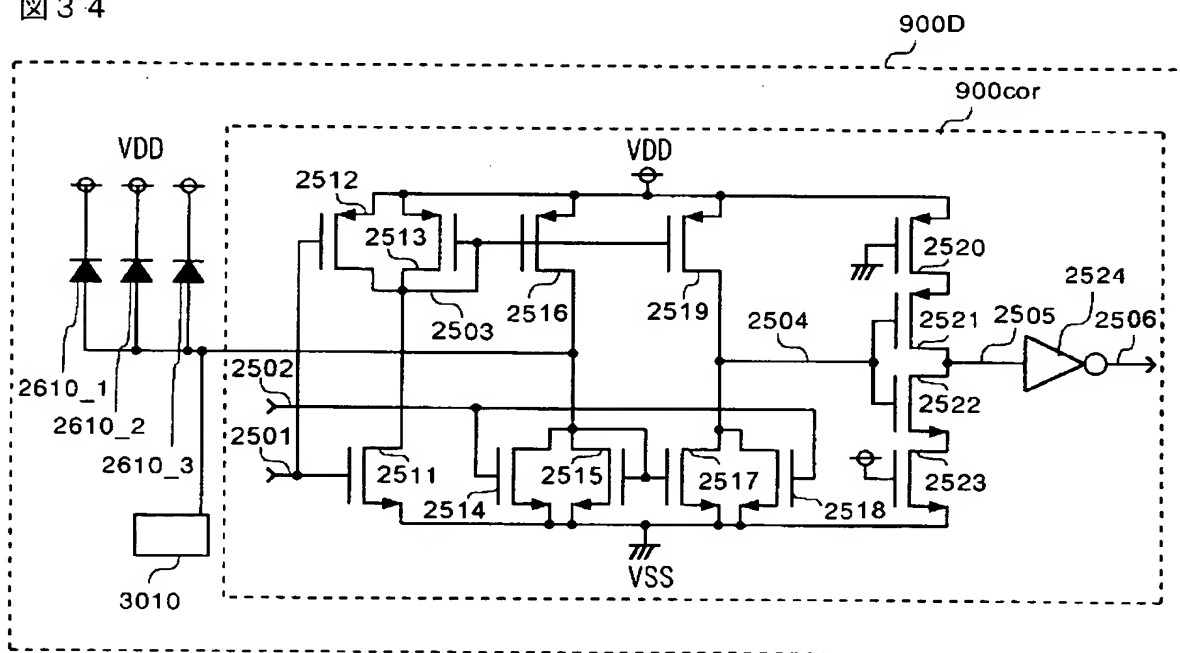
【図 3 3】

図 3 3



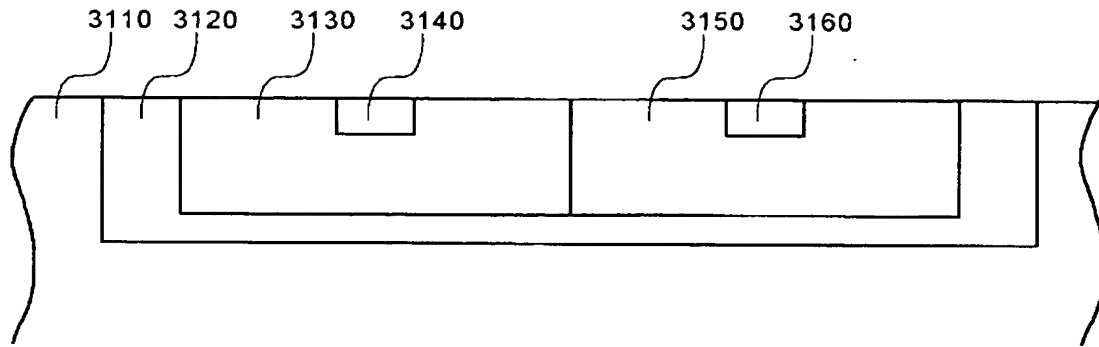
【図 3 4】

図 3 4



【図 35】

図 35



【書類名】 要約書**【要約】**

【課題】 光照射により積極的に誤動作を誘発して機密保護情報を不正に獲得するというカードハッキングに対する防御が可能な半導体集積回路を提供する。

【解決手段】 ICカードマイコンなどの半導体集積回路に対し、標準的なロジックプロセスで構成され、他の回路と区別が付きにくく、待機電力が極めて小さい、光ディテクタを搭載する。光ディテクタは例えば、初期化動作でスタティックラッチ（1 2 0）に第1状態を保持し、第1状態のスタティックラッチを構成する非導通状態の半導体素子（1 1 2, 1 1 3）に光が照射されて第2状態に反転する構成を備え、光ディテクタをメモリセルアレイに複数個配置する。スタティックラッチ型の光ディテクタをメモリアレイに組み込むことで、それを目立たずに配置することができる。光の照射によるリバースエンジニアリングを効果的に防ぐことができる。

【選択図】 図 1

特願 2 0 0 3 - 3 2 3 9 2 3

出 願 人 履 歴 情 報

識別番号

[5 0 3 1 2 1 1 0 3]

1. 変更年月日

2 0 0 3 年 4 月 1 日

[変更理由]

新規登録

住 所

東京都千代田区丸の内二丁目 4 番 1 号

氏 名

株式会社ルネサステクノロジ